DrayTek

Vigor*IPPBX* 2820-Serie

Benutzerhandbuch

Version: 2.02

Datum: 16.03.2010

Hinweise zum Urheberrecht

Angaben zum Urheberrecht

Copyright 2009 Alle Rechte vorbehalten. Diese Publikation enthält urheberrechtlich geschützte Informationen. Kein Teil hiervon darf ohne die schriftliche Genehmigung des Urheberrechtsinhabers vervielfältigt, übertragen, umgeschrieben, in einem Datenabfragesystem gespeichert oder in irgendeine Sprache übersetzt werden.

Warenzeichen

Die folgenden Warenzeichen werden in diesem Dokument verwendet:

- Microsoft ist ein eingetragenes Warenzeichen der Microsoft Corp.
- Windows, Windows 95, 98, Me, NT, 2000, XP, Vista und Explorer sind Warenzeichen der Microsoft Corp.
- Apple und Mac OS sind eingetragene Warenzeichen von Apple Inc.
- Andere Produkte können Warenzeichen oder eingetragene Warenzeichen der entsprechenden Hersteller sein.

Sicherheitshinweise und Genehmigung

Sicherheitshinweise

- Lesen Sie die Installationsanweisungen sorgfältig durch, bevor Sie den Router einrichten.
- Der Router ist ein kompliziertes elektronisches Gerät, das nur durch autorisiertes, qualifiziertes Personal repariert werden darf. Versuchen Sie nicht, den Router selbst zu öffnen oder zu reparieren.
- Stellen Sie den Router nicht an einem feuchten Ort auf (z.B. Badezimmer).
- Der Router sollte an einem geschützten Ort in einem Temperaturbereich von +5 bis +40°C betrieben werden.
- Setzen Sie den Router nicht direktem Sonnenlicht oder anderen Wärmequellen aus. Das Gehäuse und elektronische Bauteile können durch direktes Sonnenlicht oder Wärmequellen geschädigt werden.
- Um Gefahren durch elektronische Schläge zu vermeiden, setzen Sie das LAN-Verbindungskabel nicht im Außenbereich ein.
- Halten Sie die Verpackung von Kindern fern.
- Bei der Entsorgung des Routers bitte örtliche Naturschutzvorschriften beachten.

Gewährleistung

Wir garantieren dem ursprünglichen Endbenutzer (Käufer), dass der Router für einen Zeitraum von zwei (2) Jahren ab Kaufdatum frei von Herstellungs- und Werkstofffehlern sein wird. Bitte bewahren Sie Ihren Kaufbeleg gut auf, da dieser als Nachweis des Kaufdatums dient. Sollte das Produkt während des Gewährleistungszeitraums Mängel aufweisen, die auf fehlerhafter Herstellung und/oder Werkstoffen beruhen, werden wir gegen Vorlage des Kaufbelegs nach eigenem Ermessen die mangelhaften Produkte oder Bauteile ohne Berechnung von Ersatzteil- und Arbeitszeitkosten so reparieren oder ersetzen, wie wir es für notwendig erachten, um das Produkt in den einwandfreien Betriebszustand zu versetzen. Bei ersetzten Produkten handelt es sich um neue oder überarbeitete, funktional gleichwertige Produkte, die wir nach eigenem Ermessen anbieten. Die Gewährleistung gilt nicht, wenn das Produkt modifiziert, missbraucht, manipuliert, durch höhere Gewalt geschädigt oder anormalen Betriebsbedingungen ausgesetzt wird. Die Gewährleistung umfasst nicht die gebündelte oder lizenzierte Software anderer Hersteller. Mängel, welche die Gebrauchsfähigkeit des Produkts nicht wesentlich einschränken, werden durch die Gewährleistung nicht abgedeckt. Wir behalten uns vor, das Handbuch und die Online-Dokumentation zu revidieren und die Inhalte gegebenenfalls zu ändern, ohne dass wir verpflichtet wären, irgendeine Person über solche Revisionen oder Änderungen zu benachrichtigen.

Werden Sie ein registrierter Benutzer

Online-Registrierung wird empfohlen. Sie können Ihren Vigor-Router unter http://www.draytek.de registrieren.

Firmware- und Tool-Aktualisierungen

Aufgrund der ständigen Weiterentwicklung der DrayTek-Technologie werden die Router regelmäßig verbessert. Weitere Informationen zur neuesten Firmware, Tools und Dokumenten werden auf der DrayTek Web-Site vorgehalten.

http://www.draytek.de

EG-Erklärungen

Hersteller: DrayTek Corp.
Anschrift: No. 26, Fu Shing Road, HuKou Township, HsinChu Industrial Park, Hsin-Chu County, Taiwan 303
Produkt: Vigor*IPPBX* 2820

DrayTek Corp. erklärt hiermit, dass die Router der VigorIPPBX 2820-Serie den folgenden wesentlichen Anforderungen und anderen relevanten Bestimmungen der R&TTE-Richtlinie 1999/5/EG entsprechen.

Das Produkt entspricht durch Erfüllung der Anforderungen von EN55022/Klasse B und EN55024/Klasse B den Anforderungen der EMV-Richtlinie 2004/108/EG.

Das Produkt entspricht durch Erfüllung der Anforderungen von EN60950-1 den Anforderungen der Niederspannungsrichtlinie 2006/95/EG.

Aufsichtsrechtlicher Hinweis

FCC-Erklärung

Dieses Gerät wurde getestet und entspricht den Grenzwerten für digitale Geräte der Klasse B gemäß Teil 15 der FCC-Richtlinien. Diese Grenzwerte wurden definiert, um einen angemessenen Schutz gegen Funkstörungen in häuslichen Umgebungen sicherzustellen. Dieses Gerät kann Radiofrequenzenergie generieren, verwenden und ausstrahlen. Wird das Gerät nicht gemäß den Anweisungen installiert und verwendet, kann es zu Überlagerungen bei Funkübertragungen kommen. Es kann nicht garantiert werden, dass Funkstörungen bei einer bestimmten Installation nicht auftreten. Sollte dieses Gerät den Radio- oder Fernsehempfang stören, was festgestellt werden kann, indem das Gerät aus- und wieder eingeschaltet wird, ist der Benutzer angehalten, die Funkstörung durch eine der folgenden Maßnahmen zu beseitigen:

- Ausrichtung oder Standort der Empfangsantenne ändern.
- Entfernung zwischen dem Gerät und dem Empfänger vergrößern.
- Verbinden Sie das Gerät und den Empfänger mit getrennten Steckdosen bzw. Stromkreisen.
- Wenden Sie sich an den Fachhändler oder an einen erfahrenen Radio-/Fernsehtechniker.

Dieses Gerät entspricht Teil 15 der FCC-Richtlinien. Der Betrieb ist unter den folgenden zwei Bedingungen gestattet:

(1) Dieses Gerät darf keine Störungen verursachen.

(2) Dieses Gerät muss alle empfangenen Störungen , einschließlich Störungen, die einen unerwünschten Betrieb zur Folge haben, akzeptieren.

Bitte besuchen Sie http://www.draytek.com/user/AboutRegulatory.php.

Dieses Produkt ist für DSL-, ISDN- und POTS--Netzwerke in der gesamten EU und in der Schweiz sowie mit Einschränkungen in Frankreich geeignet. Die verfügbaren Netzwerke sind auf Ihrem Produkt angegeben.

Inhaltsverzeichnis

Kapitel 1: Vorwort....1

1.1 Erläuterung der Web-Konfigurationstasten....1

1.2 LED-Anzeigen und Anschlüsse....2

1.2.1 VigorIPPBX 2820....3
1.2.2 VigorIPPBX 2820n....5

1.3 Hardwareinstallation....7

1.4 Installation eines ISDN-Telefonadapters....8

1.5 Druckerinstallation....9

Kapitel 2: Grundlegende Einstellungen....14

2.1 Passwort ändern....14

2.2 Schnellstart-Assistent....16

2.2.1 PPPoE/PPPoA....17
2.2.2 1483 Bridged IP....19
2.2.3 1483 Routed IP....20

2.3 TK-Anlage-Assistent....21

2.3.1 Konfiguration der Nebenstellengruppen....21
2.3.2 Konfiguration der SIP-Amtsleitungen....22
2.3.3 Konfiguration der Tag-/Nacht-Anrufvariante....23

2.4 Onlinestatus....25

2.4 Konfiguration speichern....28

Kapitel 3: Anwendungen....29

3.1 Anmeldung von 50 IP-basierten Telefonen/Nebenstellen....29

3.2 IP-Anmeldung von entferntem Standort (über WAN-Verbindung)....30

3.3 Integration von IP-Anmeldung über SIP-Server....31

3.4 Integration von VoIP-Kommunikation über SIP-Server....32

3.5 Integration von analoger Telefonie....33

3.6 Zusätzliche ISDN-Telefonie....34

3.7 Integrierte ISDN-Leitung....35

3.8 Vier B-Kanäle der zwei ISDN-Leitungen....36

3.9 Integration einer ISDN-TK-Anlage mit einer ISDN-Leitung....37

3.10 Netzwerkaufbau (ISDN und analog)....38

3.11 Integration von ISDN-Telefonie und analogem Netzwerk....39

3.12 Integration von ISDN-Telefonie, analogem Netzwerk und VoIP-Verbindung....40

Kapitel 4: Weitere Anwendungen....41

4.1 LAN-zu-LAN-Verbindung zwischen Filiale und Zentrale einrichten....41

4.2 Einwahlverbindung zwischen externem Teleworker und Zentrale einrichten....48

4.3 Beispiel für QoS-Einstellungen....52

4.4 LAN – Einrichtung mit NAT....56

4.5 Firmware des Routers aktualisieren....57
4.6 Zertifikat von einem CA-Server oder Windows CA-Server anfordern....59
4.7 CA-Zertifikat von Windows CA-Server anfordern und als vertrauenswürdiges Zertifikat setzen....63

Kapitel 5: Referenz - erweiterte Web-Konfiguration....65

5.1 WAN....65
5.1.1 Grundlagen des Internet Protocol (IP) Netzwerks....65
5.1.2 Netzwerkverbindung über 3G USB-Modem....66
5.1.3 Basiskonfiguration....67
5.1.4 Einwahl ins Internet....70
5.1.5 Multi-PVCs....87
5.1.6 Load-Balance....92
5.2 LAN....95
5.2.1 LAN-Grundlagen....95
5.2.2 Basiskonfiguration....97
5.2.3 Feste Adressumleitung....101
5.2.4 VLAN....103
5.2.5 IP an MAC binden....105
5.3 NAT....106
5.3.1 Portumleitung....107
5.3.2 DMZ-Host....110
5.3.3 Offene Ports....112
5.4 Firewall....114
5.4.1 Firewall-Grundlagen....114
5.4.2 Basiskonfiguration....116
5.4.3 Filtereinstellung....119
5.4.4 DoS-Abwehr....127
5.5 Objekte....131
5.5.1 IP-Objekt....131
5.5.2 IP-Gruppe....133
5.5.3 Servicetyp-Objekt....134
5.5.4 Servicetyp-Gruppe....135
5.5.5 Stichwort-Objekt....136
5.5.6 Stichwort-Gruppe....137
5.5.7 Dateiformat-Objekt....138
....139
5.5.8 IM-Objekt....140
....141
5.5.9 P2P-Objekt....142
5.5.10 Diverses....143
5.6 CSM....144
5.6.1 IM-/P2P-Filter....146
5.6.2 Inhaltsbezogener URL-Filter....146
5.6.3 Inhaltsbezogener Web-Filter....151
5.7 Bandbreitenmanagement....154
5.7.1 Sitzungen begrenzen....154
5.7.2 Bandbreitenbegrenzung....155
5.7.3 QoS....157
5.8 Anwendungen....164
5.8.1 Dynamisches DNS....164

5.8.2 Verbindungstimer....166
5.8.3 RADIUS....169
5.8.4 UPnP....170
5.8.5 IGMP....172
5.8.6 Wake on LAN....173

5.9 VPN und externe Einwahl....174

5.9.1 Einwahlmöglichkeiten....174
5.9.2 PPP-Einstellungen....175
5.9.3 IPSec Grundeinstellungen....176
5.9.4 IPSec-Identität....178
5.9.5 Externe Benutzer....180
5.9.6 LAN zu LAN....184
5.9.7 Verbindungsmanagement....194

5.10 Zertifikatsverwaltung....195

5.10.1 Lokales Zertifikat....195
5.10.2 Vertrauenswürdiges CA-Zertifikat....197
5.10.3 Zertifikat sichern....198

5.11 ISDN....199

5.11.1 Grundkonzept....199
5.11.2 Basiskonfiguration....199
5.11.3 Einwahl über einen ISP....202
5.11.4 Einwahl über zwei ISPs....203
5.11.5 Verbindungseinstellungen....205

5.12 TK-Anlage....207

5.12.1 Nebenstellen....208
5.12.2 Leitungseinstellungen....211
5.12.3 Telefonbuch....217
5.12.4 System....221
5.12.5 Statusanzeige....247

5.13 Wireless LAN....248

5.13.1 Grundlagen....248
5.13.2 Basiskonfiguration....250
5.13.3 Verschlüsselung....253
5.13.4 Zugriffskontrolle....255
5.13.5 WPS....257
5.13.6 WDS....259
5.13.7 Erweiterte Einstellungen....262
5.13.8 Liste der Access Points....264
5.13.9 Liste der Clients....265

5.14 Systemmanagement....266

5.14.1 Systemstatus....266
5.14.2 TR-069....267
5.14.3 Administratorpasswort....268
5.14.4 Sicherung der Konfiguration....269
5.14.5 Syslog/Mail-Alarm....270
5.14.6 Zeit und Datum....272
5.14.7 Verwaltung....273
5.14.8 Neustart....275
5.14.9 Firmware aktualisieren....275

5.15 Diagnose-Tools....277

5.15.1 Anwahlauslöser....277
5.15.2 Routing-Tabelle....278
5.15.3 ARP-Cache-Tabelle....278

5.15.4 DHCP-Tabelle....279
5.15.5 NAT-Sitzungstabelle....280
5.15.6 Ping....280
5.15.7 Datenfluss-Monitor....281
5.15.8 Traffic-Diagramm....283
5.15.9 Trace Route....284

Kapitel 6: Fehlersuche....285

6.1 Hardwarestatus überprüfen....285
6.2 Netzwerkeinstellungen am PC kontrollieren....286
6.3 Pingen des Routers von Ihrem PC aus....288
6.4 Prüfen der ISP-Einstellungen....289
6.5 Probleme mit der 3G-Netzwerkverbindung....292
6.6 Auf Werkseinstellungen zurücksetzen (Factory-Reset)....293
6.7 Technische Hilfe....294

Anhang: Technische Daten....295

Kapitel 1: Vorwort

Der VigorIPPBX 2820 ist ein ADSL- und Breitband-Router mit WAN-Schnittstelle. Der Router bietet Policy-gesteuerte Lastverteilung (Load Balance), Failover und BOD (Bandwidth on Demand) sowie QoS auf IP-Ebene und NAT Sitzungs-/Bandbreitenmanagement, um bei großen Bandbreiten effektive Benutzerkontrolle zu ermöglichen.

Durch den Einsatz der hardwarebasierten VPN-Plattform und AES/DES/3DS-Hardwareverschlüsselung steigert der Router die VPN-Leistung enorm und bietet verschiedene Protokolle (wie IPSec/PPTP/L2TP) mit bis zu 32 VPN-Tunneln.

Das objektbasierte Konzept, das in der SPI-Firewall (Stateful Packet Inspection) verwendet wird, erleichtert Benutzern die Einrichtung der Firewall-Regeln. CSM (Content Security Management) gibt Benutzern effizientere Kontrolle im Umgang mit IM (Instant Messenger) und P2P (Peer to Peer). DoS/DDoS-Schutz und inhaltsbezogene URL-/Web-Filter verbessern die externe Sicherheit und die interne Kontrolle.

VigorIPPBX 2820 unterstützt bis zu 50 Nebenstellen, womit alle angemeldeten IP-Telefone im LAN oder an entfernten Standorten weltweit von den Vorteilen der Internet-Telefonie profitieren können. Ferner ermöglicht der VigorIPPBX 2820 die Einrichtung mehrerer Netzwerkarchitekturen, um sowohl Ihren aktuellen Wünschen als auch Ihren zukünftigen wachsenden Kommunikationsbedürfnissen zu entsprechen. Dank seiner Kompatibilität mit dem ISDN- und dem analogen Telefonnetz können Sie nach Bedarf einfache VoIP-Lösungen wie IP-Telefone und Softphones mit anderen Netzwerktechnologien wie ISDN und analogem Telefon kombinieren.

Die objektbasierte Firewall ist flexibel und macht Ihr Netzwerk sicher. Durch die VoIP-Funktion können Sie und Ihre Gesprächspartner Kommunikationskosten sparen.

1.1 Erläuterung der Web-Konfigurationstasten

In den Dialogen werden die folgenden Schaltflächen häufig verwendet:

OK:	Speichert und wendet Einstellungen an.
Abbrechen:	Die aktuellen Eingaben werden gelöscht.
Löschen:	Fügt für die ausgewählte Funktion neue Einstellungen hinzu.
Hinzufügen:	Neue Einstellungen werden hinzugefügt.
Bearbeiten:	Bearbeitet die ausgewählte Funktion.
Alles löschen:	Der ausgewählte Eintrag wird mit allen Einstellungen gelöscht.

Hinweis: Die anderen in den Dialogen angezeigten Schaltflächen werden in Kapitel 4 detailliert erläutert.

1.2 LED-Anzeigen und Anschlüsse

Bevor Sie den Vigor-Router verwenden, machen Sie sich bitte mit den LED-Anzeigen und Anschlüssen vertraut.

Die LED-Anzeigen und Anschlüsse der Router unterscheiden sich geringfügig. Diese werden in den folgenden Abschnitten vorgestellt. Falls Ihr Router-Modell ISDN und/oder VoIP nicht unterstützt, ignorieren Sie einfach die entsprechende Beschreibung.

Definitionen für ISDN-Ports

Die Bezeichnungen an der Vorderseite des Gerätes und in der Web-Oberfläche sind wie folgt:

ISDN1 und **ISDN2** an der Vorderseite des Gerätes können gemäß Ihren Einstellungen in der Web-Oberfläche als Telefon- oder Internetverbindung genutzt werden.

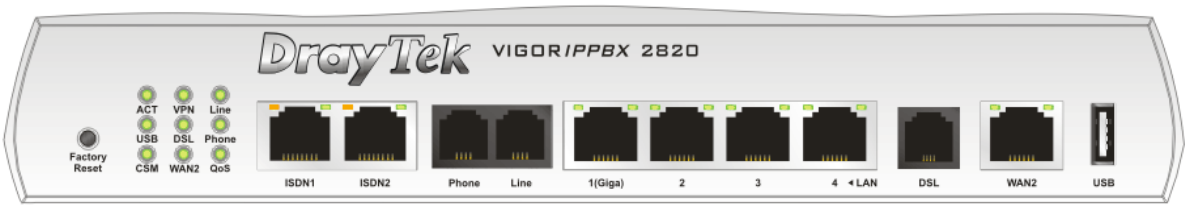
ISDN1-TE /ISDN2-TE (in der Web-Oberfäche) ist ein Port für den ISDN-Anschluss.

ISDN1-S0/ISDN2-S0 (in der Web-Oberfläche) ist ein Port für das ISDN-Telefon.

Detaillierte Informationen sind im Benutzerhandbuch unter **TK-Anlage>>System>>Telefoneinstellungen** verfügbar.

Warnung: Wenn die orangefarbene LED aufleuchtet (ISDN NT Modus), kann der ISDN-Port nur zum Anschließen eines Telefonapparates verwendet werden. Eine falsche ISDN-Verbindung kann Ihren Router ernsthaft beschädigen.

1.2.1 VigorIPPBX 2820

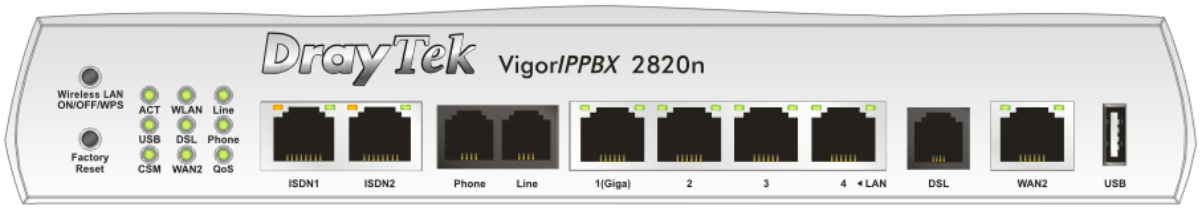


LED	Status	Erläuterung
ACT (Aktivität)	Blinkt	Der Router ist eingeschaltet und funktioniert ordnungsgemäß.
	Aus	Der Router ist ausgeschaltet.
USB	Ein	Ein USB-Gerät ist angeschlossen und aktiv.
	Blinkt	Es werden Daten übertragen.
CSM	Ein	Das CSM-Profil (Content Security Management) für IM-/P2P-Anwendungen kann unter **Firewall >>Basiskonfiguration** aktiviert werden. (Das eigentliche Profil muss im **CSM**-Menü eingerichtet werden.)
VPN	Ein	VPN-Tunnel ist an/aus.
DSL	Ein	Der Router ist bereit für die Einwahl ins Internet über den DSL-Link.
	Blinkt	Langsam: Das Modem ist bereit. Schnell: Die Verbindung wird angepasst.
WAN 2	Ein	Die WAN 2-Verbindung ist bereit.
	Blinkt	Es werden Daten übertragen.
Line	Ein	Ein- oder ausgehender PSTN-Anruf. Wenn der Anruf beendet wird, erlischt die LED nach ca. sechs Sekunden.
	Aus	Kein PSTN-Telefonanruf
Phone	Ein	Das an diesem Port angeschlossene Telefon wurde abgenommen.
	Aus	Das an diesem Port angeschlossene Telefon ist aufgelegt.
	Blinkt	Eingehender Anruf
QoS	Ein	Die QoS-Funktion ist aktiv.
LED am Anschluss		
ISDN1/2Linke LED (orange)	Ein	Zeigt an, dass der unter **TK-Anlage>>System>>Telefoneinstellungen** konfigurierte ISDN S0 (ISDN-NT) Modus aktiv ist und ein ISDN-Telefonadapter angeschlossen ist.
	Blinkt	Zeigt an, dass der unter **TK-Anlage>>System>>Telefoneinstellungen** konfigurierte ISDN S0 (ISDN-NT) Modus aktiv ist und kein ISDN-Telefonadapter angeschlossen ist.
	Aus	Zeigt an, dass der unter **TK-Anlage>>System>>Telefoneinstellungen** konfigurierte ISDN TE Modus aktiv ist.
Rechte LED (grün)	Ein	Zeigt an, dass ein Telefonadapter mit Telefonapparat (ISDN-S0) oder eine ISDN-Amtsleitung (ISDN-TE) angeschlossen ist.
	Blinkt	ISDN-S0 (ISDN-NT) Modus; zeigt an, dass ein ISDN-Telefon abgenommen wurde oder ein eingehender Anruf ansteht. ISDN-TE Modus; zeigt an, dass Sprache (Telefonanruf), Fax oder Daten übertragen werden.
	Aus	Ist aus, falls nichts angeschlossen ist.
LAN 1 (Giga)Linke LED (grün)	Ein	Der Port ist verbunden.
	Aus	Der Port ist nicht verbunden.
	Blinkt	Es werden Daten übertragen.
Rechte LED (grün)	Ein	Der Port ist mit 1000 Mbit/s verbunden.
	Aus	Der Port ist mit 10/100 Mbit/s verbunden.
LAN	Ein	Der Port ist verbunden.

2/3/4Linke LED (grün)	Aus	Der Port ist nicht verbunden.
	Blinkt	Es werden Daten übertragen.
Rechte LED (grün)	Ein	Der Port ist mit 100 Mbit/s verbunden.
	Aus	Der Port ist mit 10 Mbit/s verbunden.
WAN 2Linke LED (grün)	Ein	Der Port ist verbunden.
	Aus	Der Port ist nicht verbunden.
	Blinkt	Es werden Daten übertragen.
Rechte LED (grün)	Ein	Der Port ist mit 100 Mbit/s verbunden.
	Aus	Der Port ist mit 10 Mbit/s verbunden.

Schnittstelle	Erläuterung
Vorderseite	
Wireless LAN ON/OFF/WPS	Durch einmaliges Drücken des WLAN-Knopfes können Sie die WLAN-Verbindung ein- (LED an) oder ausschalten (LED aus). Halten Sie den WLAN-Knopf zwei Sekunden lang gedrückt, um es Clients zu ermöglichen, über WPS eine Netzwerkverbindung aufzubauen.
Factory Reset	Auf Werkseinstellungen zurücksetzen Anwendung: Schalten Sie den Router an (die ACT LED blinkt). Drücken Sie den versenkten Taster länger als 10 Sekunde. Wenn die ACT-LED beginnt, schneller als normal zu blinken, kann die Taste losgelassen werden. Jetzt wird der Vigor mit den Werkseinstellungen neu gestartet.
Phone S0	Schnittstelle für ISDN-Telefone (NUR mit ISDN-Telefonadapter betreiben, da beim Anschluss anderer Kabel der Router schwer beschädigt werden kann!)
ISDN/ Phone S0	Schnittstelle für die ISDN-Amtsleitung (NTBA, ISDN-TK-Anlage) oder ISDN-Telefon je nach Konfiguration (siehe Abschnitt 2.2)
Phone1/2	Schnittstellen für den Anschluss von analogen Telefonen
Line	Schnittstelle für den Anschluss der analogen Amtsleitung.
LAN 1-4	Schnittstellen für lokale Netzwerkgeräte
DSL	Schnittstelle für die Internetverbindung über das integrierte ADSL2/2+Modem
WAN2	Schnittstelle für Modems und Router zur Internetverbindung
USB	Schnittstelle für den Anschluss eines 3G USB-Modems oder eines Druckers
Rückseite	
PWR	Netzteilanschluss
ON/OFF	An/-Ausschalter

1.2.2 VigorIPPBX 2820n



LED	Status	Erläuterung
ACT (Aktivität)	Blinkt	Der Router ist eingeschaltet und funktioniert ordnungsgemäß.
	Aus	Der Router ist ausgeschaltet.
USB	Ein	Ein USB-Gerät ist angeschlossen und aktiv.
	Blinkt	Es werden Daten übertragen.
CSM	Ein	Das CSM-Profil (Content Security Management) für IM-/P2P-Anwendungen kann unter **Firewall >>Basiskonfiguration** aktiviert werden. (Das eigentliche Profil muss im **CSM**-Menü eingerichtet werden.)
WLAN	Ein	Der Wireless Access Point ist bereit.
	Blinkt	Blinkt während dem Wireless-Datenverkehr. Blinken die ACT- und WLAN-LEDs gleichzeitig, wurde der WPS-Modus aktiviert, und WLAN-Clients können sich via WPS mit dem Vigor synchronisieren. (WPS muss innerhalb von 2 Minuten eingerichtet werden.)
DSL	Ein	Der Router ist bereit für die Einwahl ins Internet über den DSL-Link.
	Blinkt	Langsam: Das Modem ist bereit. Schnell: Die Verbindung wird angepasst.
WAN 2	Ein	Die WAN 2-Verbindung ist bereit.
	Blinkt	Es werden Daten übertragen.
Line	Ein	Ein- oder ausgehender PSTN-Anruf. Wenn der Anruf beendet wird, erlischt die LED nach ca. sechs Sekunden.
	Aus	Kein PSTN-Telefonanruf aktiv
Phone	Ein	Das an diesem Port angeschlossene Telefon wurde abgenommen.
	Aus	Das an diesem Port angeschlossene Telefon ist aufgelegt.
	Blinkt	Eingehender Anruf
QoS	Ein	Die QoS-Funktion ist aktiv.
LED am Anschluss		
ISDN1/2 Linke LED (orange)	Ein	Zeigt an, dass der unter **TK-Anlage>>System>>Telefoneinstellungen** konfigurierte ISDN S0 (ISDN-NT) Modus aktiv ist und ein ISDN-Telefonadapter angeschlossen ist.
	Blinkt	Zeigt an, dass der unter **TK-Anlage>>System>>Telefoneinstellungen** konfigurierte ISDN S0 (ISDN-NT) Modus aktiv ist und kein ISDN-Telefonadapter angeschlossen ist.
	Aus	Zeigt an, dass der unter **TK-Anlage>>System>>Telefoneinstellungen** konfigurierte ISDN TE Modus aktiv ist.
Rechte LED (grün)	Ein	Zeigt an, dass ein Telefonadapter mit Telefonapparat (ISDN-S0) oder eine ISDN-Amtsleitung (ISDN-TE) angeschlossen ist.
	Blinkt	ISDN-S0 (ISDN-NT) Modus; zeigt an, dass ein ISDN-Telefon abgenommen wurde oder ein eingehender Anruf ansteht. ISDN-TE Modus; zeigt an, dass Sprache (Telefonanruf), Fax oder Daten übertragen werden.
	Aus	Ist aus, falls nichts angeschlossen ist.
LAN 1 (Giga)Link	Ein	Der Port ist verbunden.
	Aus	Der Port ist nicht verbunden.

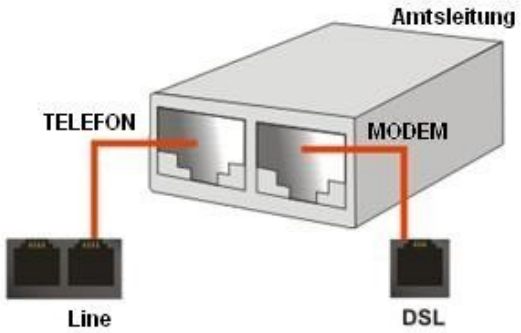
e LED (grün)	Blinkt	Es werden Daten übertragen.
Rechte LED (grün)	Ein	Der Port ist mit 1000 Mbit/s verbunden.
	Aus	Der Port ist mit 10/100 Mbit/s verbunden.
LAN 2/3/4Linke LED (grün)	Ein	Der Port ist verbunden.
	Aus	Der Port ist nicht verbunden.
	Blinkt	Es werden Daten übertragen.
Rechte LED (grün)	Ein	Der Port ist mit 100 Mbit/s verbunden.
	Aus	Der Port ist mit 10 Mbit/s verbunden.
WAN 2Linke LED (grün)	Ein	Der Port ist verbunden.
	Aus	Der Port ist nicht verbunden.
	Blinkt	Es werden Daten übertragen.
Rechte LED (grün)	Ein	Der Port ist mit 100 Mbit/s verbunden.
	Aus	Der Port ist mit 10 Mbit/s verbunden.

Schnittstelle	Erläuterung
Vorderseite	
Wireless LAN ON/OFF/WPS	Durch einmaliges Drücken des WLAN-Knopfes können Sie die WLAN-Verbindung ein- (LED an) oder ausschalten (LED aus). Halten Sie den WLAN-Knopf zwei Sekunden lang gedrückt, um es Clients zu ermöglichen, über WPS eine Netzwerkverbindung aufzubauen.
Factory Reset	Auf Werkseinstellungen zurücksetzen Anwendung: Schalten Sie den Router an (die ACT LED blinkt). Drücken Sie den versenkten Taster länger als 10 Sekunde. Wenn die ACT-LED beginnt, schneller als normal zu blinken, kann die Taste losgelassen werden. Jetzt wird der Vigor mit den Werkseinstellungen neu gestartet.
Phone S0	Schnittstelle für ISDN-Telefone (NUR mit ISDN-Telefonadapter betreiben, da beim Anschluss anderer Kabel der Router schwer beschädigt werden kann!)
ISDN/ Phone S0	Schnittstelle für die ISDN-Amtsleitung (NTBA, ISDN-TK-Anlage) oder ISDN-Telefon je nach Konfiguration (siehe Abschnitt 2.2)
Phone1/2	Schnittstellen für den Anschluss von analogen Telefonen
Line	Schnittstelle für den Anschluss der analogen Amtsleitung.
LAN 1-4	Schnittstellen für lokale Netzwerkgeräte
DSL	Schnittstelle für die Internetverbindung über das integrierte ADSL2/2+Modem
WAN2	Schnittstelle für Modems und Router zur Internetverbindung
USB	Schnittstelle für den Anschluss eines 3G USB-Modems oder eines Druckers
Rückseite	
PWR	Netzteilanschluss

1.3 Hardwareinstallation

Bevor Sie den Router konfigurieren, müssen Sie Ihre Geräte ordnungsgemäß anschließen.

1. Verbinden Sie die ADSL-Schnittstelle mit Hilfe des ADSL-Kabels mit dem externen ADSL-Splitter. Verbinden Sie auch die Line-Schnittstelle mit dem externen ADSL-Splitter.



Für eine zweite WAN-Verbindung verbinden Sie das Kabelmodem/DSL-Modem/Medienkonverter über ein Ethernet-Kabel (RJ-45) mit dem WAN2-Port des Routers.

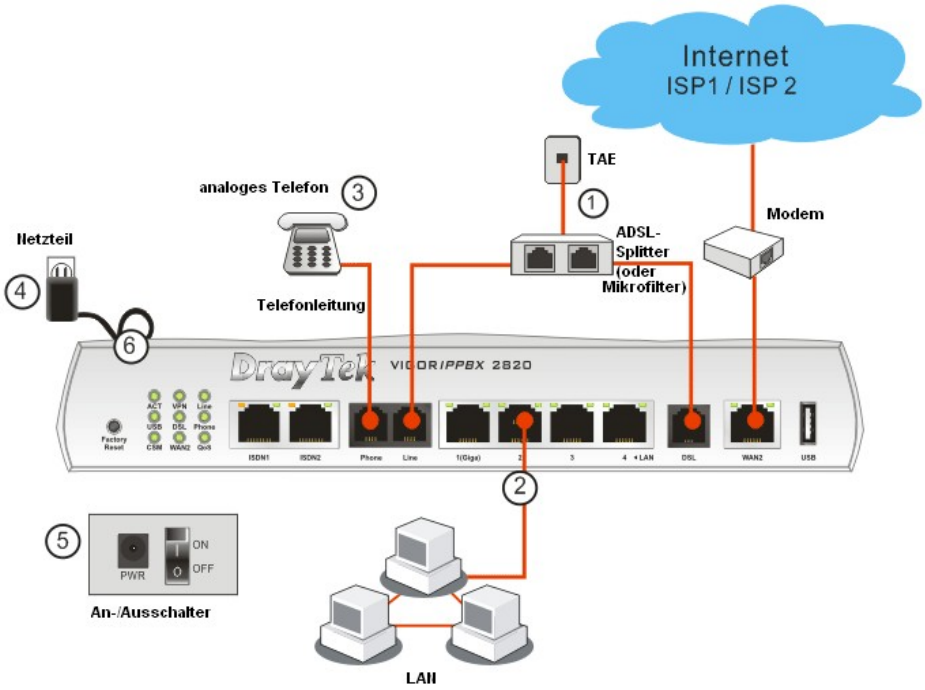
2. Verbinden Sie ein Ende eines Ethernet-Kabels (RJ-45) mit einem der **LAN**-Ports am Router und das andere Ende des Kabels (RJ-45) mit dem Ethernet-Port Ihres Rechners.Verbinden Sie den Telefonapparat mit Hilfe eines Telefonkabels (um die VoIP-Funktion zu verwenden). Beim Modell ohne Telefonanschluss überspringen Sie diesen Schritt.

3. Verbinden Sie den Ausgang des Netzteils mit dem Netzanschluss auf der Rückseite und das andere Ende mit einer Steckdose.

4. Schalten Sie das Gerät ein, indem Sie auf den Netzschalter auf der Rückseite drücken.

5. Das System wird initialisiert. Nach Abschluss des Systemtests leuchtet die **ACT** LED auf und fängt an, zu blinken.

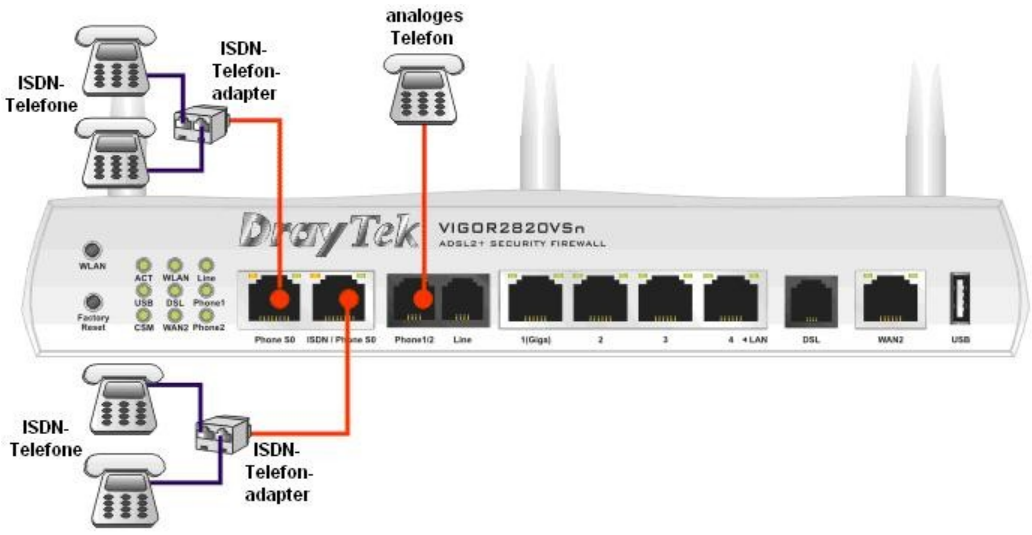
(Einzelheiten zum LED-Status werden in Abschnitt 1.2 erläutert.)



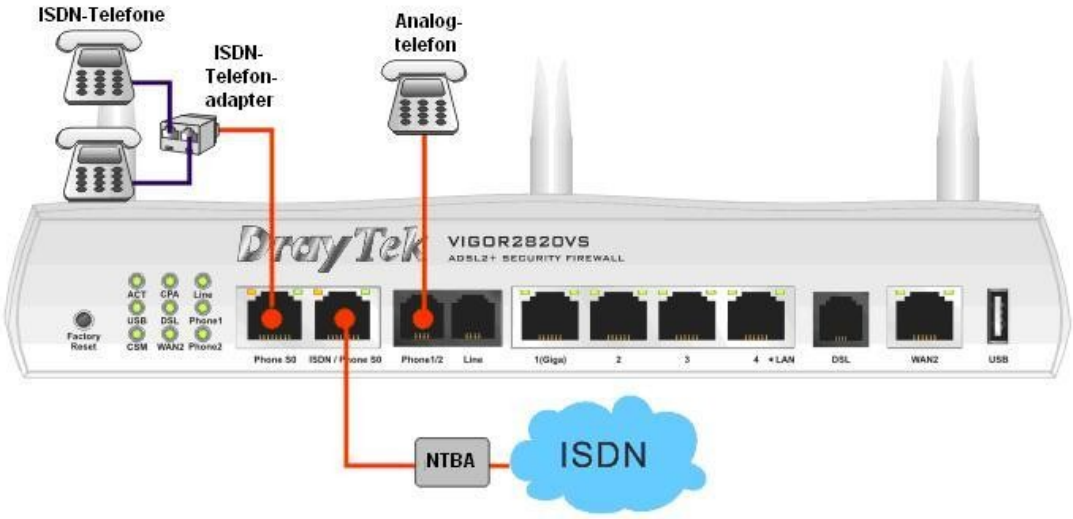
Achtung: Jeder Telefonanschluss darf nur mit einem analogen Telefon verbunden werden. Verbinden Sie die Telefonanschlüsse nicht mit der Telefonsteckdose. Eine solche Verbindung kann Ihren Router beschädigen.

1.4 Installation eines ISDN-Telefonadapters

Die ISDN-Ports 1 und 2 können für den NT- oder TE-Modus konfiguriert werden. Konfiguriert der Benutzer den ISDN-Port unter **TK-Anlage>>System>>Telefoneinstellungen** für den NT-Modus, so leuchtet die **orangefarbene** LED auf, um anzuzeigen, dass **ISDN-NT** ausgewählt ist. Durch Nutzung des ISDN-Telefonadapters (im Lieferumfang enthalten) kann der Benutzer mehrere Telefonapparate an den Router anschließen. Die folgende Abbildung zeigt eine beispielhafte Konstellation.



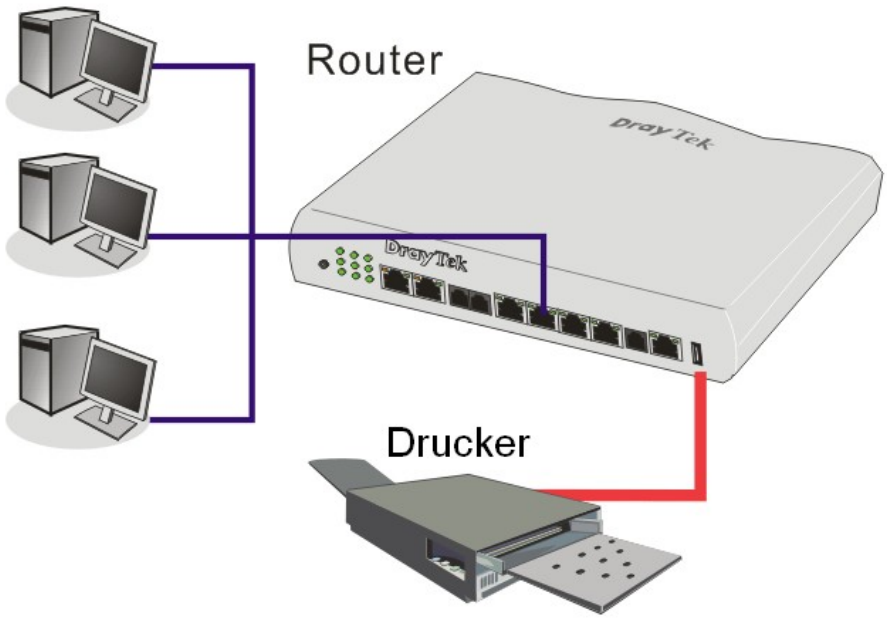
Konfiguriert der Benutzer den ISDN-Port unter **TK-Anlage>>System>>Telefoneinstellungen** hingegen für den TE-Modus, so leuchtet die **grüne** LED auf, um anzuzeigen, dass **ISDN-TE** ausgewählt ist. Dementsprechend ist der Port nur für die ISDN-Amtsleitung bestimmt. Die folgende Abbildung zeigt eine beispielhafte Konstellation.



1.5 Druckerinstallation

Sie können mit dem Router einen Netzwerkdrucker installieren. Alle an diesem Router angeschlossenen Rechner können über den Router drucken. Das hier gezeigte Beispiel verwendet Windows XP.

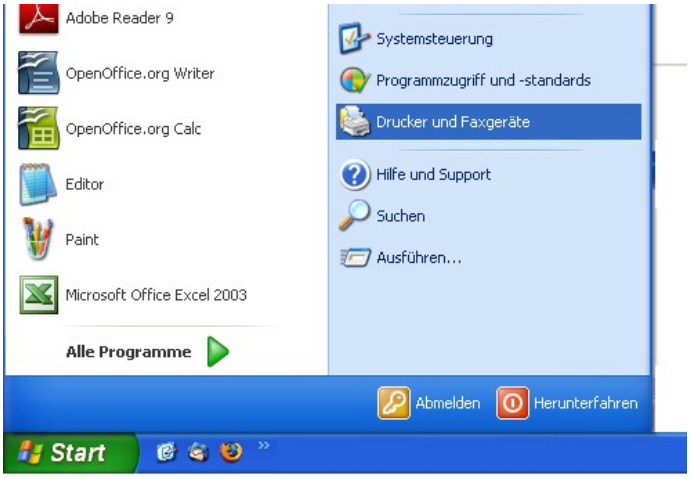
Druckername: 192.168.1.1
Portname: IP_192.168.1.1



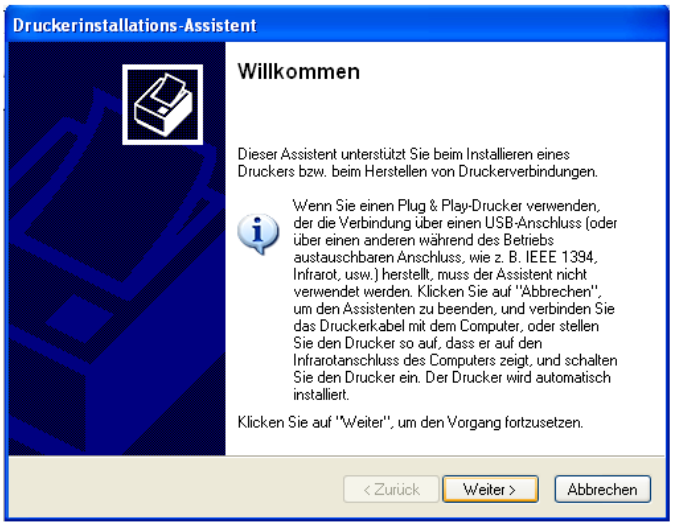
Bevor Sie den Drucker verwenden, konfigurieren Sie die angeschlossenen Rechner (oder Wireless-Clients) bitte wie folgt.

1. Verbinden Sie den Drucker über die USB-/parallele Schnittstelle mit dem Router.

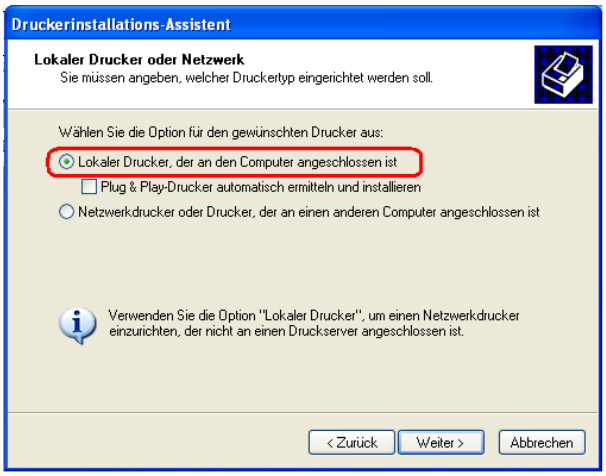
2. Öffnen Sie **Start → Systemsteuerung → Drucker und Faxgeräte**.



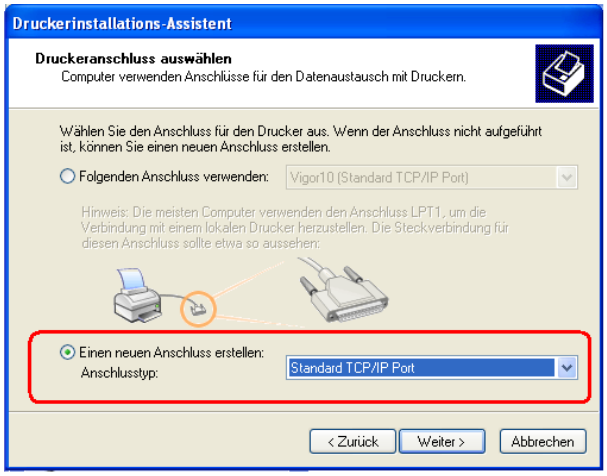
4. Öffnen Sie **Datei → Drucker hinzufügen**. Der Druckerinstallations-Assistent erscheint. Klicken Sie auf **Weiter**.


Druckerinstallations-Assistent
Willkommen
Dieser Assistent unterstützt Sie beim Installieren eines Druckers bzw. beim Herstellen von Druckerverbindungen.
Wenn Sie einen Plug & Play-Drucker verwenden, der die Verbindung über einen USB-Anschluss (oder über einen anderen während des Betriebs austauschbaren Anschluss, wie z. B. IEEE 1394, Infrarot, usw.) herstellt, muss der Assistent nicht verwendet werden. Klicken Sie auf "Abbrechen", um den Assistenten zu beenden, und verbinden Sie das Druckerkabel mit dem Computer, oder stellen Sie den Drucker so auf, dass er auf den Infrarotanschluss des Computers zeigt, und schalten Sie den Drucker ein. Der Drucker wird automatisch installiert.
Klicken Sie auf "Weiter", um den Vorgang fortzusetzen.
< Zurück
Weiter >
Abbrechen

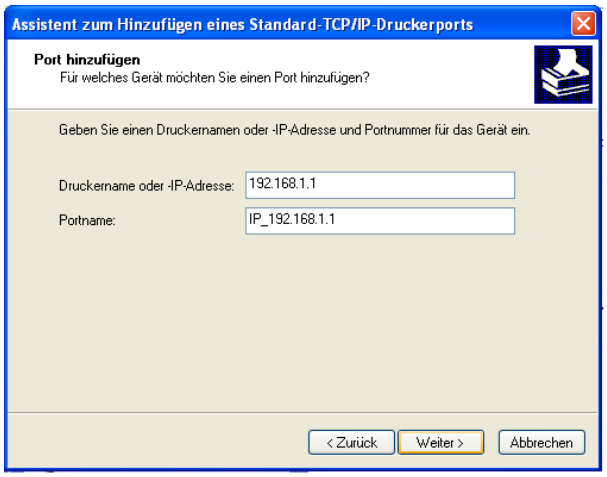
5. Klicken Sie auf "Lokaler Drucker, der an den Computer angeschlossen ist".


Druckerinstallations-Assistent
Lokaler Drucker oder Netzwerk
Sie müssen angeben, welcher Druckertyp eingerichtet werden soll.
Wählen Sie die Option für den gewünschten Drucker aus:
Lokaler Drucker, der an den Computer angeschlossen ist
Plug & Play-Drucker automatisch ermitteln und installieren
Netzwerkdrucker oder Drucker, der an einen anderen Computer angeschlossen ist
Verwenden Sie die Option "Lokaler Drucker", um einen Netzwerkdrucker einzurichten, der nicht an einen Druckserver angeschlossen ist.
< Zurück
Weiter >
Abbrechen

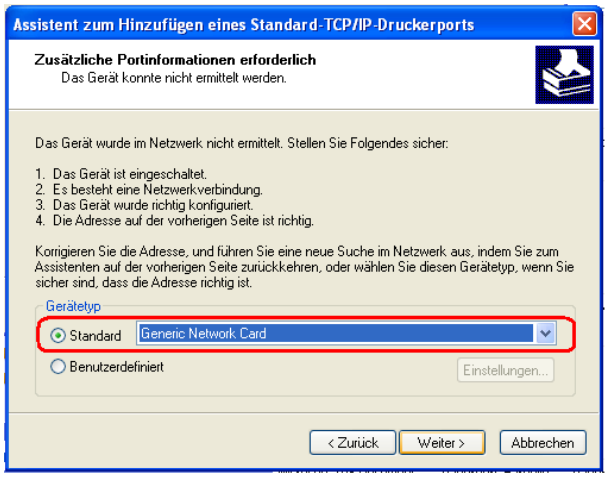
6. Wählen Sie in diesem Dialog **Einen neuen Anschluss erstellen** und markieren Sie in der Dropdown-Liste **Standard TCP/IP Port**. Klicken Sie auf **Weiter**.


Druckerinstallations-Assistent
Druckeranschluss auswählen
Computer verwenden Anschlüsse für den Datenaustausch mit Druckern.
Wählen Sie den Anschluss für den Drucker aus. Wenn der Anschluss nicht aufgeführt ist, können Sie einen neuen Anschluss erstellen.
Folgenden Anschluss verwenden:
Vigor10 (Standard TCP/IP Port)
Hinweis: Die meisten Computer verwenden den Anschluss LPT1, um die Verbindung mit einem lokalen Drucker herzustellen. Die Steckverbindung für diesen Anschluss sollte etwa so aussehen:
Einen neuen Anschluss erstellen:
Anschlusstyp:
Standard TCP/IP Port
< Zurück
Weiter >
Abbrechen

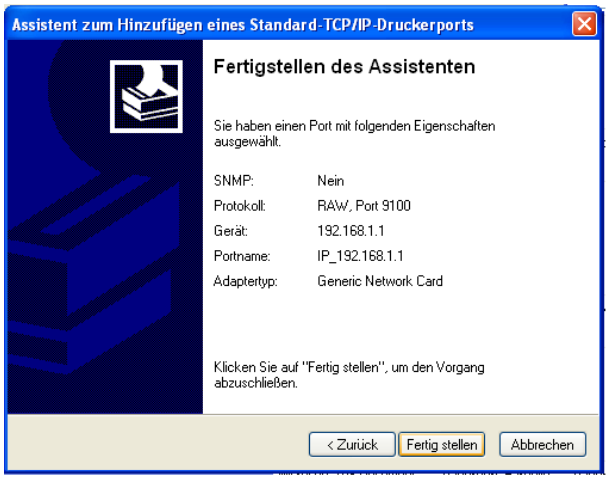
7. Geben Sie im folgenden Dialog im Feld **Druckername oder -IP-Adresse** die LAN IP-Nummer des Routers **192.168.1.1** und im Feld **Portname** die Bezeichnung **IP_192.168.1.1** ein. Klicken Sie dann auf **Weiter**.



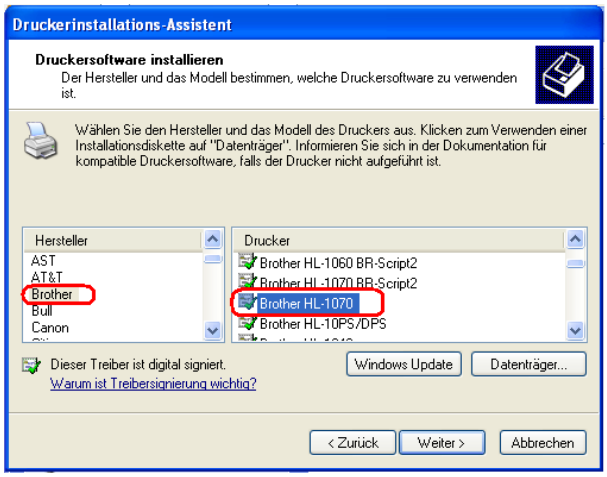
8. Markieren Sie "Standard" und wählen Sie "Generic Network Card".


Assistent zum Hinzufügen eines Standard-TCP/IP-Druckerports
Zusätzliche Portinformationen erforderlich
Das Gerät konnte nicht ermittelt werden.
Das Gerät wurde im Netzwerk nicht ermittelt. Stellen Sie Folgendes sicher:
1. Das Gerät ist eingeschaltet.
2. Es besteht eine Netzwerkverbindung.
3. Das Gerät wurde richtig konfiguriert.
4. Die Adresse auf der vorherigen Seite ist richtig.
Korrigieren Sie die Adresse, und führen Sie eine neue Suche im Netzwerk aus, indem Sie zum Assistenten auf der vorherigen Seite zurückkehren, oder wählen Sie diesen Gerätetyp, wenn Sie sicher sind, dass die Adresse richtig ist.
Gerätetyp
Standard
Generic Network Card
Benutzerdefiniert
Einstellungen...
< Zurück
Weiter >
Abbrechen

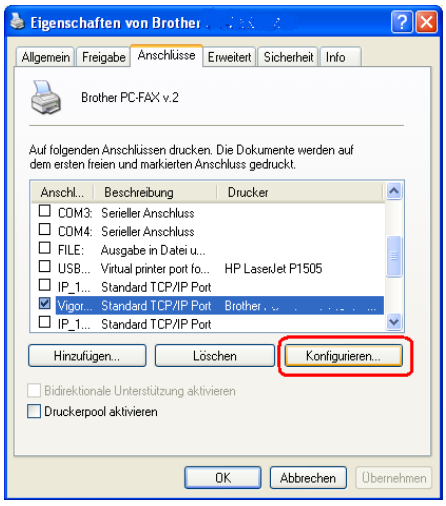
9. Klicken Sie im folgenden Dialog auf **Fertig stellen**.



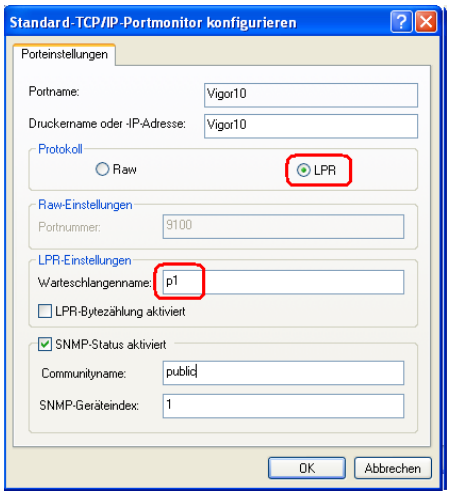
10. Nun wählen Sie Hersteller und das Modell des Druckers, den Sie an Ihrem Router angeschlossen haben. Durch diesen Schritt wird der richtige Treiber installiert.



11. Abschließend müssen Sie in das Menü **Systemsteuerung-> Drucker und Faxgeräte** zurückkehren und die Eigenschaften des neu hinzugefügten Druckers bearbeiten.



12. Wählen Sie als **LPR** als Protokoll und geben Sie **p1** (Nummer 1) als Warteschlangenname ein. Klicken Sie dann auf **OK**. Die entsprechenden Einstellungen sind in der Abbildung rot umrandet.



Der Drucker kann jetzt zum Drucken verwendet werden. Die meisten Drucker verschiedener Hersteller sind mit dem Vigor-Router kompatibel.

Hinweis 1: Einige Drucker mit Fax-/Scanner- oder anderen Zusatzfunktionen werden nicht unterstützt. Falls Sie sich nicht sicher sind, ob Ihr Drucker unterstützt wird, prüfen Sie bitte die Druckerliste unter www.draytek.com (**Support->FAQ->Printer Server->What types of printers are compatible with Vigor router?)**.

Der Vigor-Router nimmt Druckaufträge von Rechnern über LAN-Ports an, nicht aber über den WAN-Port.

Kapitel 2: Grundlegende Einstellungen

Um den Router ordnungsgemäß zu verwenden, ändern Sie zu Ihrer Sicherheit das Web-Konfigurationspasswort und passen Sie die Grundeinstellungen an.

Dieses Kapitel erklärt, wie Sie ein Administratorpasswort einrichten, die grundlegenden Einstellungen für die Einwahl ins Internet erfolgreich anpassen, und die Einstellungen für die TK-Anlage mit Hilfe des Assistenten konfigurieren können. Beachten Sie, dass die Router-Konfiguration nur durch den Administrator geändert werden kann.

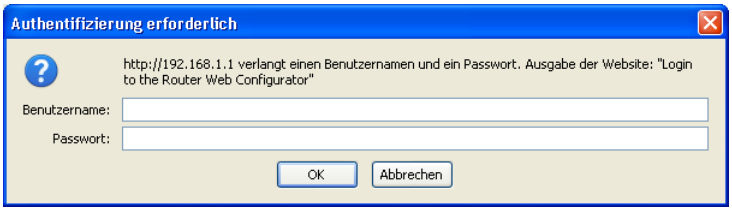
2.1 Passwort ändern

Um das Passwort für dieses Gerät zu ändern, müssen Sie sich zunächst mit dem voreingestellten Passwort im Web-Browser anmelden.

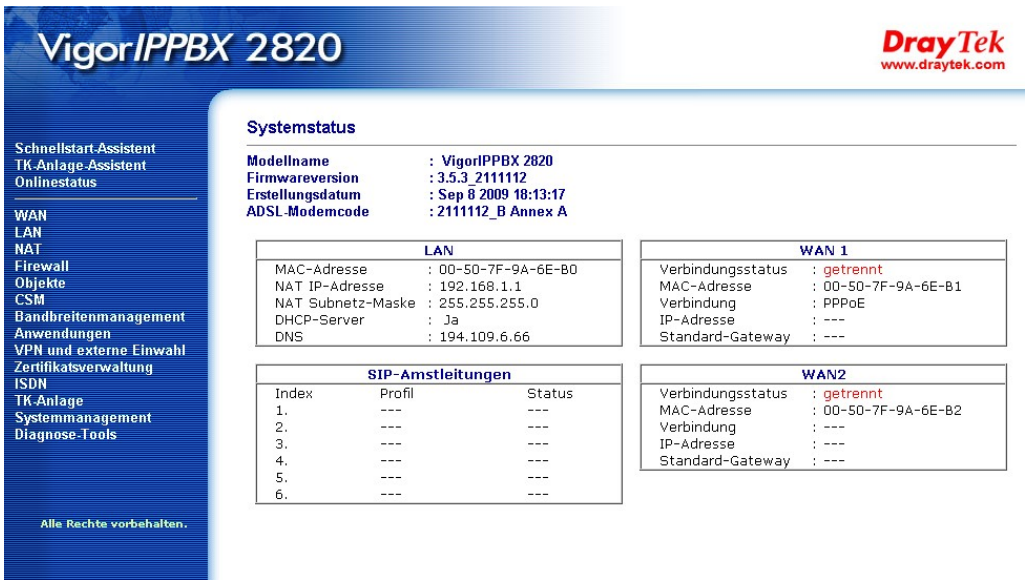
1. Sorgen Sie dafür, dass Ihr Computer richtig mit dem Router verbunden ist.

> **Hinweis:** Sie können Ihren Rechner so konfigurieren, dass die IP dynamisch vom Router zugewiesen wird, oder eine IP-Adresse aus dem gleichen Subnetz wählen, in dem sich **die Standard-IP-Adresse des Vigor-Routers befindet (192.168.1.1)**. Einzelheiten hierzu werden im Abschnitt "Fehlerbehandlung" weiter hinten im Handbuch beschrieben.

2. Öffnen Sie auf Ihrem PC einen Web-Browser und geben Sie **http://192.168.1.1** ein. Ein Popup-Fenster erscheint und fragt Sie nach Ihrem Benutzernamen und Passwort. Geben Sie als Benutzernamen "admin" ein und lassen Sie das Passwort leer. Klicken Sie auf **OK**, um zur nächsten Maske zu gelangen.

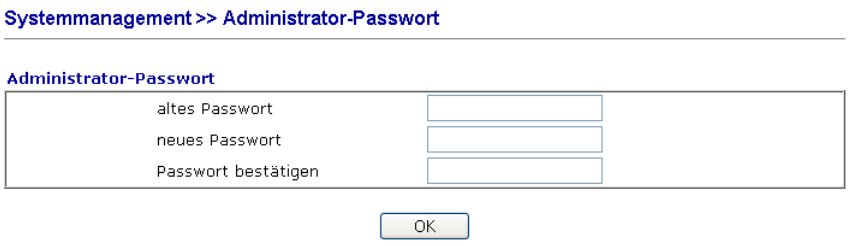


3. Das **Hauptfenster** erscheint.



Anmerkung: Die Startseite kann sich je nach Router-Modell leicht unterscheiden.

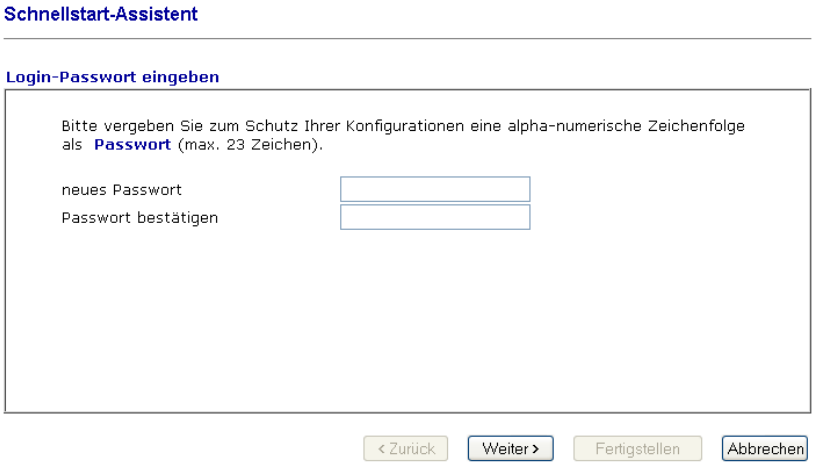
4. Gehen Sie zu **Systemmanagement** und wählen Sie **Administratorpasswort**.



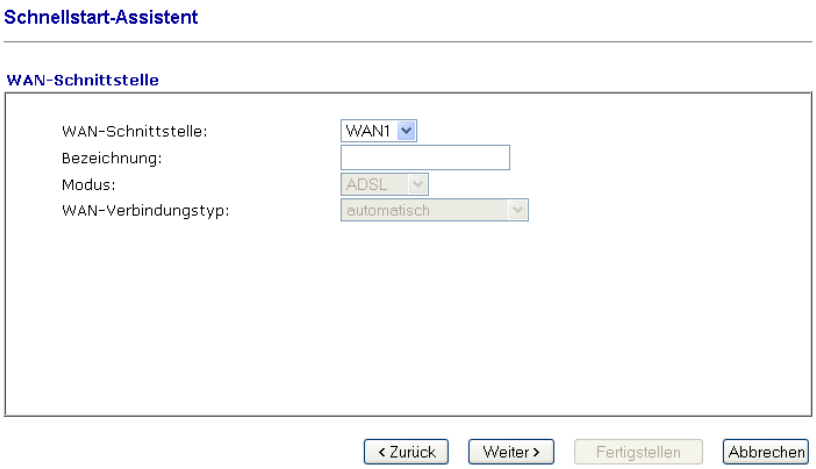
5. Geben Sie das Anmeldepasswort (standardmäßig leer) im Feld **Altes Passwort** ein. Geben Sie ein **Neues Passwort** ein. Klicken Sie dann auf **OK**, um fortzufahren.
6. Das Passwort ist nun geändert worden. Verwenden Sie beim nächsten Mal das neue Passwort, um auf das Menü des Routers zuzugreifen.

2.2 Schnellstart-Assistent

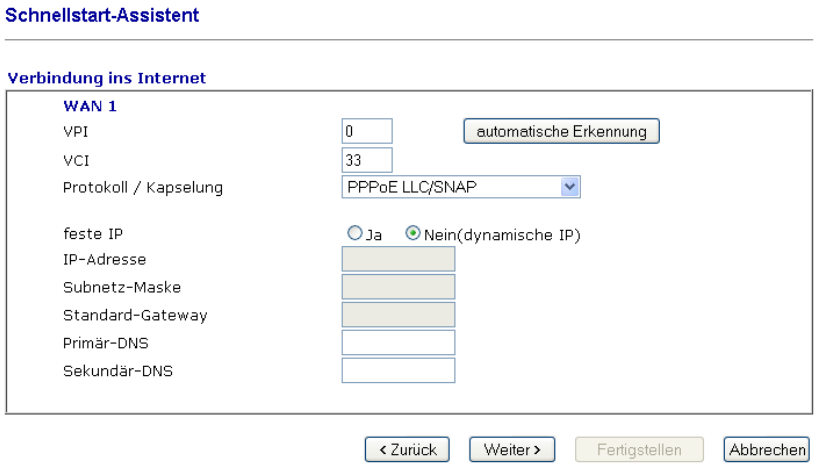
Die hier beschriebene Konfiguration wird Sie dabei unterstützen, Ihren Router schnell für Breitband-DSL einzurichten und zu verwenden. Das erste Dialogfenster des **Schnellstart-Assistenten** erfordert die Eingabe des Anmeldepassworts. Geben Sie das Passwort ein und klicken auf **Weiter**.

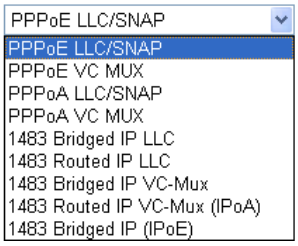


Auf der nächsten Seite (siehe unten) wählen Sie bitte die verwendete WAN-Schnittstelle (WAN1 oder WAN2). Falls Sie DSL verwenden, um eine Internetverbindung herzustellen, wählen Sie bitte WAN1; für die Anbindung eines externen Modems mit Ethernetschnittstelle wählen Sie WAN2. Bestimmen Sie als Verbindungstyp **Automatisch**. Dann klicken Sie auf **Weiter**, um zum nächsten Schritt zu gelangen.



Auf der nächsten Seite (siehe unten) wählen Sie die richtige Art der Einwahl ins Internet gemäß den Informationen von Ihrem ISP. So wählen Sie zum Beispiel den PPPoE-Modus, falls Ihr ISP dies unterstützt. Dann klicken Sie auf **Weiter**, um zum nächsten Schritt zu gelangen.





Im **Schnellstart-Assistenten** können Sie den Router über verschiedene Protokolle/Modi wie **PPPoE**/**PPPoA**, **1483 Bridged IP** oder **1483 Routed IP** für die Einwahl ins Internet konfigurieren. Der Router verbindet sich über die DSL-WAN- oder die WAN2-Schnittstelle mit dem Internet.

2.2.1 PPPoE/PPPoA

PPPoE ist die Abkürzung für **Point-to-Point Protocol over Ethernet**. Dieses Protokoll verwendet zwei weit verbreitete Standards: PPP und Ethernet. Es verbindet Benutzer per Ethernet über einen gemeinsamen DSL-Anschluss, ein Wireless-Gerät oder ein Kabelmodem mit dem Internet. Alle Benutzer, die über Ethernet verbunden sind, können den Anschluss gemeinsam nutzen.

Die meisten Benutzer eines DSL-Modems verwenden PPPoE. Alle lokalen Benutzer können eine PPPoE-Verbindung für die Einwahl ins Internet gemeinsam nutzen. Sie erhalten die Informationen zum Benutzernamen, Passwort und Authentifizierungsmodus von Ihrem Internetanbieter.

Falls Ihr ISP die Verbindung über **PPPoE** anbietet, wählen Sie bitte für diesen Router **PPPoE**. Die folgende Seite erscheint:

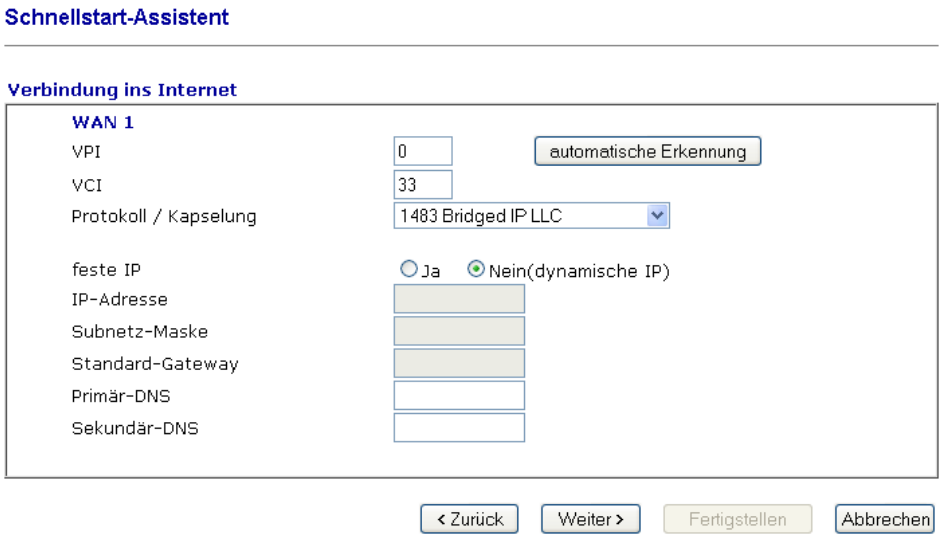
Benutzername	Geben Sie den von Ihrem ISP mitgeteilten gültigen Benutzernamen ein.
Passwort	Geben Sie das von Ihrem ISP mitgeteilte gültige Passwort ein.
Passwort bestätigen	Passwort erneut eingeben.

Klicken Sie auf **Weiter**, um die Zusammenfassung Ihrer Verbindungseinstellungen zu kontrollieren.

Klicken Sie auf **Fertigstellen**. Die Meldung **Einstellungen des Schnellstart-Assistenten werden übernommen!** erscheint. Der Systemstatus wird angezeigt.

2.2.2 1483 Bridged IP

Wählen Sie **1483 Bridged IP** als Protokoll. Geben Sie alle Daten ein, die Ihnen Ihr ISP für dieses Protokoll mitgeteilt hat.

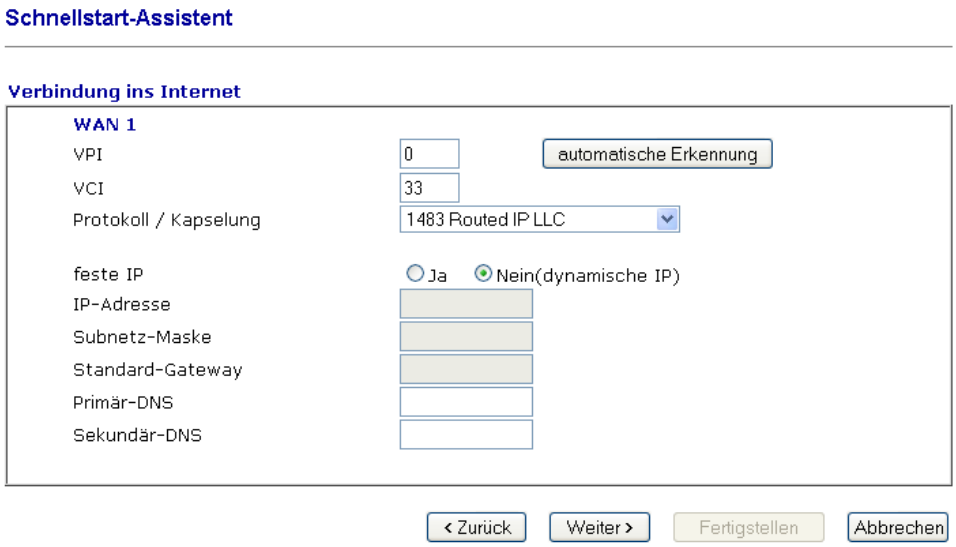


Klicken Sie auf **Weiter**, um die Zusammenfassung Ihrer Verbindungseinstellungen zu kontrollieren.

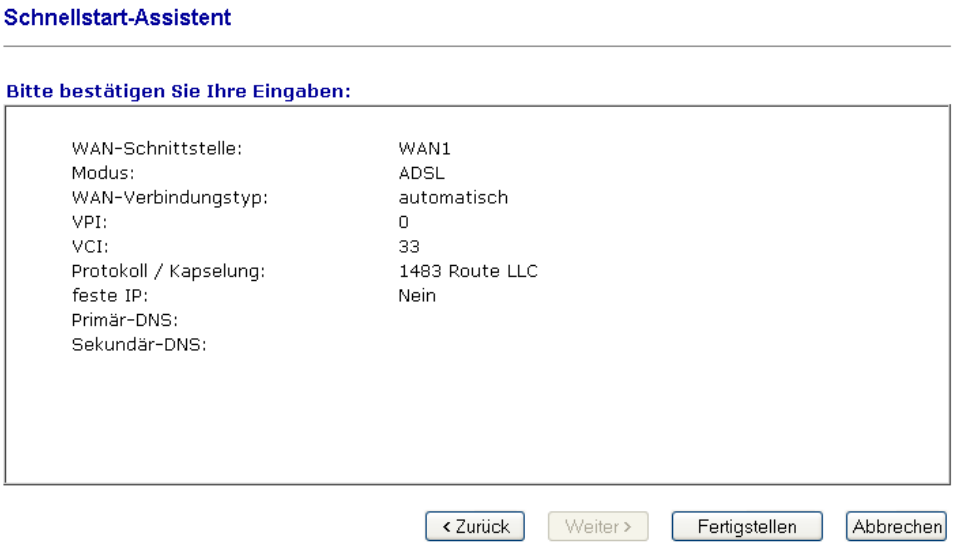
Klicken Sie auf **Fertigstellen**. Die Meldung **Einstellungen des Schnellstart-Assistenten werden übernommen!** erscheint. Der Systemstatus wird angezeigt.

2.2.3 1483 Routed IP

Wählen Sie **1483 Routed IP** als Protokoll. Geben Sie alle Daten ein, die Ihnen Ihr ISP für dieses Protokoll mitgeteilt hat.



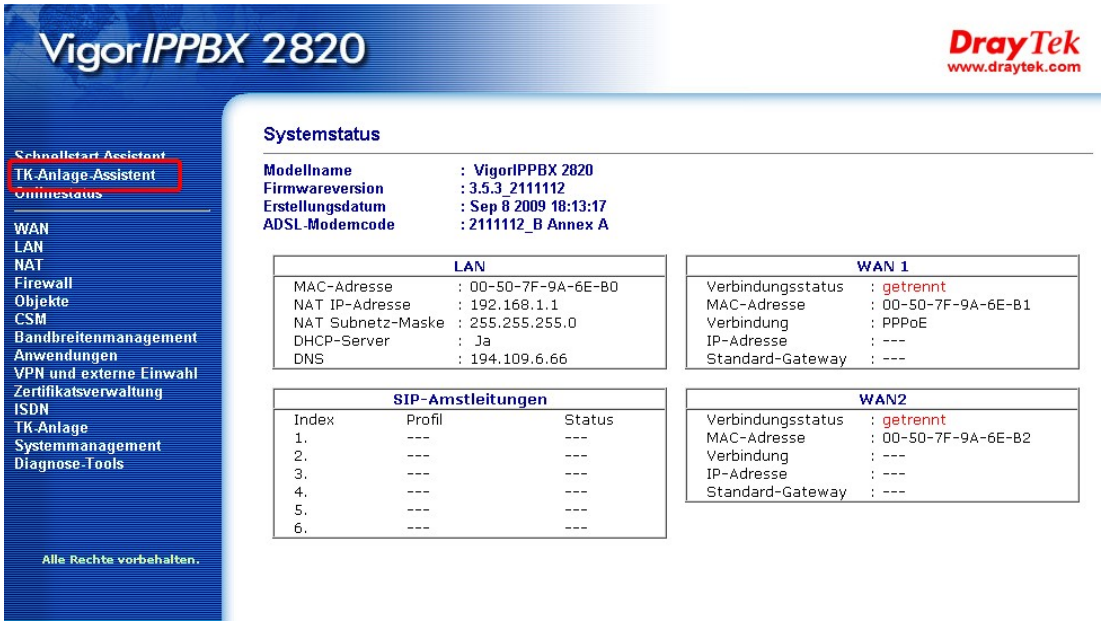
Nach Abschluss der Einstellungen auf dieser Seite klicken Sie auf **Weiter**, um zur folgenden Seite zu gelangen.



Klicken Sie auf **Fertigstellen**. Die Meldung **Einstellungen des Schnellstart-Assistenten werden übernommen!** erscheint. Der Systemstatus wird angezeigt.

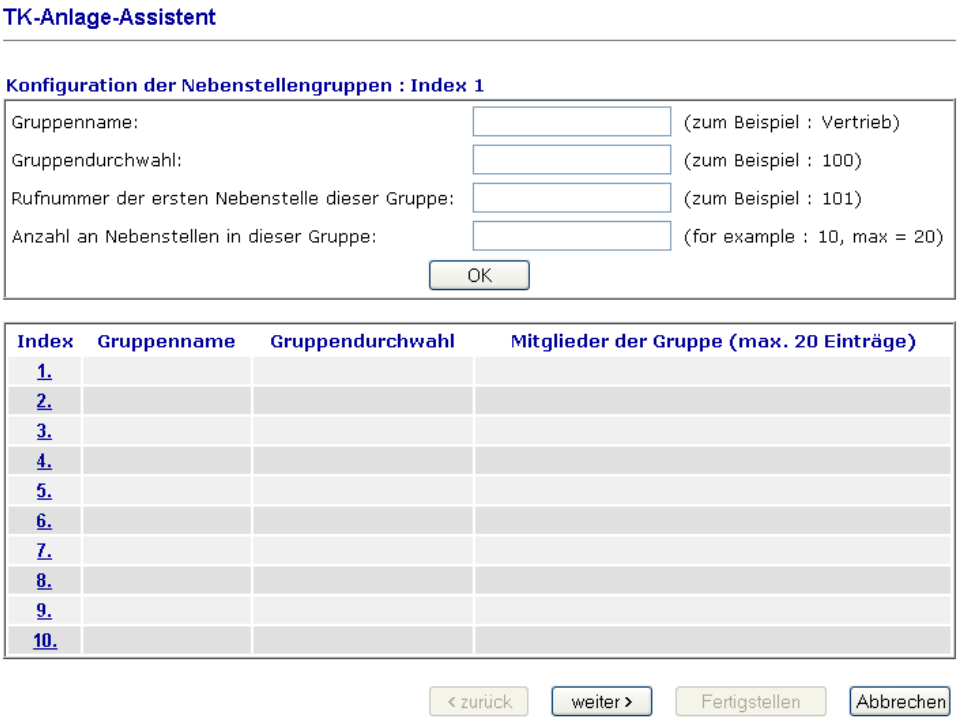
2.3 TK-Anlage-Assistent

Der-TK-Anlage-Assistent hilft dem Benutzer, die erforderlichen Einstellungen schrittweise zu konfigurieren. Sämtliche Einstellungen können auch im Menü **TK-Anlage** konfiguriert werden. Die Verwendung des Assistenten stellt jedoch für Benutzer die praktischste und einfachste Lösung dar.



2.3.1 Konfiguration der Nebenstellengruppen

Klicken Sie auf **TK-Anlage-Assistent**. Sie gelangen auf die folgende Seite:



Gruppenname - Geben Sie den anzuzeigenden Namen für diese Nebenstellengruppe ein.

Gruppendurchwahl - Geben Sie die Durchwahl der Gruppe ein.

Rufnummer der ersten Nebenstelle dieser Gruppe - Geben Sie die Rufnummer der ersten Nebenstelle dieser Gruppe ein.

Anzahl an Nebenstellen in dieser Gruppe - Geben Sie die Gesamtanzahl der Nebenstellen in der Gruppe an.

Nach Abschluss der Einstellungen in den Feldern für Gruppenname, Gruppendurchwahl, Rufnummer der ersten Nebenstelle und Anzahl an Nebenstellen klicken Sie auf **OK**, um diese zu speichern. Die neu hinzugefügte Gruppe wird auf dem Bildschirm angezeigt. Sie können 10 Gruppen für verschiedene Situationen einrichten. Dann klicken Sie auf **Weiter**, um auf die nächste Seite zu gelangen.

2.3.2 Konfiguration der SIP-Amtsleitungen

Auf dieser Seite können Sie bis zu sechs SIP-Amtsleitungen einrichten.

Profilname - Geben Sie für dieses Profil eine Bezeichnung zur Identifizierung ein.

Domain/Bereich - Setzen Sie hier den Domain-Namen oder die IP-Adresse des SIP-Registrar-Servers.

Proxy - Setzen Sie den Domain-Namen oder die IP-Adresse des SIP-Proxy-Servers. Sie können nach dem Domain-Namen die Port-Nummer in der Form **:Port-Nummer** angeben, um den entsprechenden Port als Ziel der Datenübertragung zu bestimmen (z.B. **nat.draytel.org:5065**).

Kontobezeichnung/-nummer - Geben Sie die SIP-Kontobezeichnung ein, d.h. den Text vor @.

Passwort - Das Passwort, das Ihnen im Zuge der Anmeldung bei einem SIP-Dienst mitgeteilt wurde.

Amtsnummer - Eine Nebenstelle kann auf zweierlei Weise auf die Amtsleitung zugreifen. Der erste Ansatz besteht darin, die Nummer für die Amtsleitung zu wählen und etwas zu warten. Sobald das Amtszeichen ertönt, kann die tatsächliche externe Telefonnummer gewählt werden. Alternativ kann die Nummer für die Amtsleitung und dann die tatsächliche externe Rufnummer gewählt werden, ohne auf das Amtszeichen zu warten. Die Nummer für die Amtsleitung wird als Amtsnummer bezeichnet.

Nach Abschluss der Einstellungen in den Feldern für Profilname, Domain/Bereich, Proxy, Kontobezeichnung/-nummer, Passwort und Amtsnummer klicken Sie bitte auf **OK**, um diese zu speichern. Das neu hinzugefügte Profil wird auf dem Bildschirm angezeigt.

Index	Profilname	Domäne/Realm	Proxy	Kontobezeichnung/-nummer	Amtsnummer
1.	Verkauf	192.168.1.55	net.draytel.org:5065	Verkauf	001
2.					002
3.					003
4.					004
5.					005
6.					006

< zurück | weiter > | Fertigstellen | Abbrechen

Sie können sechs Profile für unterschiedliche Bedingungen einrichten. Dann klicken Sie auf **Weiter**, um auf die nächste Seite zu gelangen.

2.3.3 Konfiguration der Tag-/Nacht-Anrufvariante

Auf dieser Seite können Sie die Tag-/Nacht-Anrufvarianten mit Startzeit und Endzeit an Arbeitstagen konfigurieren.

TK-Anlage-Assistent

Konfiguration der Tag-/Nacht-Anrufvariante

Stellen Sie hier ein, zu welchen Zeiten Sie die verschiedenen Anrufvarianten nutzen möchten.

	Stunde	Minuten
Ab wieviel Uhr soll die Tagschaltung aktiviert werden?	00	00
Soll eine Mittagsruhe eingetragen werden?	00	00
Wann ist die Mittagsruhe beendet?	00	00
Um wieviel Uhr soll die Nachtschaltung aktiviert werden?	00	00
Soll diese Zeitsteuerung auch am Wochenende aktiv sein?	○ Ja	◉ Nein

< zurück | weiter > | Fertigstellen | Abbrechen

Ab wieviel Uhr soll die Tagschaltung aktiviert werden - Verwenden Sie das Dropdown-Menü, um die Startzeit am Morgen zu bestimmen.

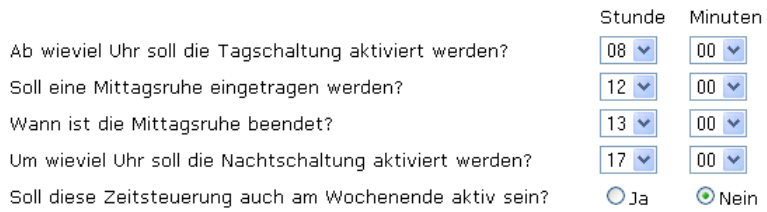
Soll eine Mittagsruhe eingetragen werden - Verwenden Sie das Dropdown-Menü, um die Endzeit am Morgen zu bestimmen.

Wann ist die Mittagsruhe beendet - Verwenden Sie das Dropdown-Menü, um die Startzeit am Nachmittag zu bestimmen.

Um wieviel Uhr soll die Nachtschaltung aktiviert werden - Verwenden Sie das Dropdown-Menü, um die Endzeit am Nachmittag zu bestimmen.

Soll diese Zeitsteuerung auch am Wochenende aktiv sein - Falls die Zeitsteuerung auch am Wochende aktiv sein soll, klicken Sie einfach auf **Ja**; andernfalls klicken Sie auf **Nein**.

Nach Abschluss der Einstellungen klicken Sie auf **Fertigstellen**, um die Einstellungen zu speichern und den Assistenten zu verlassen.



2.4 Onlinestatus

Der Onlinestatus zeigt den Systemstatus, den WAN-Status, ADSL-Informationen und andere Statusinformationen für den Router auf einer Seite an. Falls Sie **PPPoE/PPPoA** als Protokoll wählen, enthält der Dialog, der den Onlinestatus anzeigt, einen Link für **PPPoE wählen** oder **PPPoE trennen**.

Onlinestatus für PPPoE (WAN2)

Online Status

System Status — System Uptime: 3:18:44

Primary | Secondary

LAN Status — Primary DNS: 192.168.66.1 — Secondary DNS: 168.95.1.1

IP Address	TX Packets	RX Packets
192.168.1.1	749	552

WAN 1 Status — >> Release

Enable	Line	Name	Mode	Up Time	
Yes	ADSL		DHCP Client	0:00:00	
IP	**GW IP**	**TX Packets**	**TX Rate(Bps)**	**RX Packets**	**RX Rate(Bps)**
192.168.66.10	192.168.66.1	1	9	1	0

WAN 2 Status — >> Drop PPPoE

Enable	Line	Name	Mode	Up Time	
Yes	Ethernet		PPPoE	0:00:22	
IP	**GW IP**	**TX Packets**	**TX Rate(Bps)**	**RX Packets**	**RX Rate(Bps)**
218.160.234.238	61.216.116.254	14	16	15	41

ADSL Information (ADSL Firmware Version: 211011_A)

ATM Statistics	TX Blocks	RX Blocks	Corrected Blocks	Uncorrected Blocks
	18	23	0	0

ADSL Status	Mode	State	Up Speed	Down Speed	SNR Margin	Loop Att.
	G.DMT	SHOWTIME	1024000	11936000	0	0

Onlinestatus für PPPTP (für WAN2)

Online Status

System Status — System Uptime: 3:18:44

Primary | Secondary

LAN Status — Primary DNS: 168.95.1.1 — Secondary DNS: 168.95.1.1

IP Address	TX Packets	RX Packets
192.168.1.1	480	339

WAN 1 Status

Enable	Line	Name	Mode	Up Time	
Yes	ADSL		Static IP	0:00:00	
IP	**GW IP**	**TX Packets**	**TX Rate(Bps)**	**RX Packets**	**RX Rate(Bps)**
192.168.66.52	192.168.66.1	1	9	1	16

WAN 2 Status — >> Release

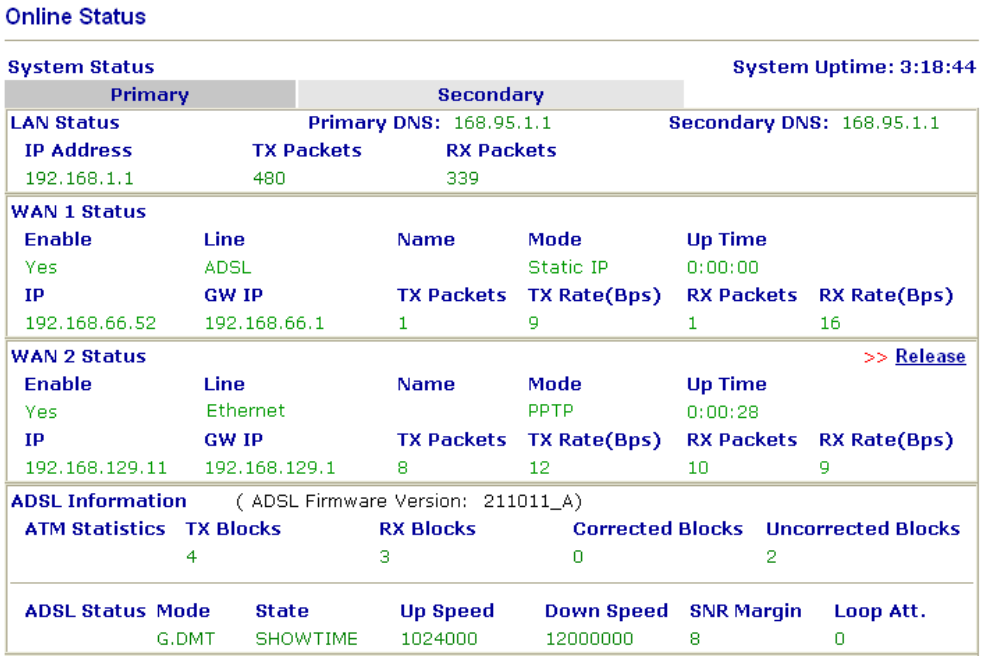
Enable	Line	Name	Mode	Up Time	
Yes	Ethernet		PPTP	0:00:28	
IP	**GW IP**	**TX Packets**	**TX Rate(Bps)**	**RX Packets**	**RX Rate(Bps)**
192.168.129.11	192.168.129.1	8	12	10	9

ADSL Information (ADSL Firmware Version: 211011_A)

ATM Statistics	TX Blocks	RX Blocks	Corrected Blocks	Uncorrected Blocks
	4	3	0	2

ADSL Status	Mode	State	Up Speed	Down Speed	SNR Margin	Loop Att.
	G.DMT	SHOWTIME	1024000	12000000	8	0

Onlinestatus für feste IP (für WAN1)



Online Status

System Status — System Uptime: 3:18:44

Primary	Secondary

LAN Status — Primary DNS: 168.95.1.1 — Secondary DNS: 168.95.1.1

IP Address	TX Packets	RX Packets
192.168.1.1	480	339

WAN 1 Status

Enable	Line	Name	Mode	Up Time	
Yes	ADSL		Static IP	0:00:00	
IP	**GW IP**	**TX Packets**	**TX Rate(Bps)**	**RX Packets**	**RX Rate(Bps)**
192.168.66.52	192.168.66.1	1	9	1	16

WAN 2 Status — >> Release

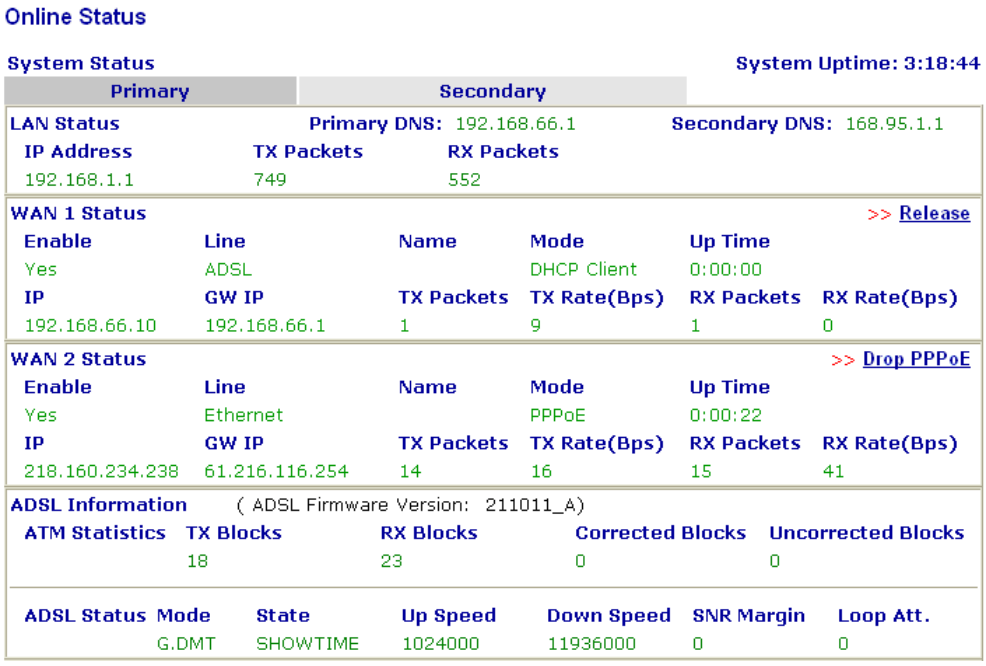
Enable	Line	Name	Mode	Up Time	
Yes	Ethernet		PPTP	0:00:28	
IP	**GW IP**	**TX Packets**	**TX Rate(Bps)**	**RX Packets**	**RX Rate(Bps)**
192.168.129.11	192.168.129.1	8	12	10	9

ADSL Information (ADSL Firmware Version: 211011_A)

ATM Statistics	TX Blocks	RX Blocks	Corrected Blocks	Uncorrected Blocks
	4	3	0	2

ADSL Status	Mode	State	Up Speed	Down Speed	SNR Margin	Loop Att.
	G.DMT	SHOWTIME	1024000	12000000	8	0

Onlinestatus für DHCP (WAN1)



Online Status

System Status — System Uptime: 3:18:44

Primary	Secondary

LAN Status — Primary DNS: 192.168.66.1 — Secondary DNS: 168.95.1.1

IP Address	TX Packets	RX Packets
192.168.1.1	749	552

WAN 1 Status — >> Release

Enable	Line	Name	Mode	Up Time	
Yes	ADSL		DHCP Client	0:00:00	
IP	**GW IP**	**TX Packets**	**TX Rate(Bps)**	**RX Packets**	**RX Rate(Bps)**
192.168.66.10	192.168.66.1	1	9	1	0

WAN 2 Status — >> Drop PPPoE

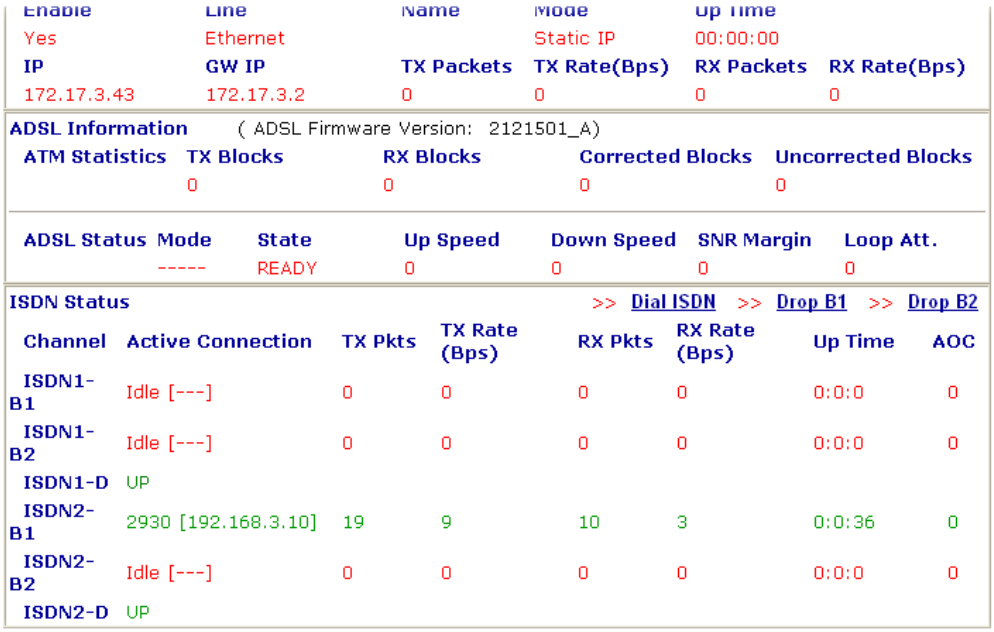
Enable	Line	Name	Mode	Up Time	
Yes	Ethernet		PPPoE	0:00:22	
IP	**GW IP**	**TX Packets**	**TX Rate(Bps)**	**RX Packets**	**RX Rate(Bps)**
218.160.234.238	61.216.116.254	14	16	15	41

ADSL Information (ADSL Firmware Version: 211011_A)

ATM Statistics	TX Blocks	RX Blocks	Corrected Blocks	Uncorrected Blocks
	18	23	0	0

ADSL Status	Mode	State	Up Speed	Down Speed	SNR Margin	Loop Att.
	G.DMT	SHOWTIME	1024000	11936000	0	0

Onlinestatus für ISDN-Modelle



Enable	Line	Name	Mode	Up Time	
Yes	Ethernet		Static IP	00:00:00	
IP	**GW IP**	**TX Packets**	**TX Rate(Bps)**	**RX Packets**	**RX Rate(Bps)**
172.17.3.43	172.17.3.2	0	0	0	0

ADSL Information (ADSL Firmware Version: 2121501_A)

ATM Statistics	TX Blocks	RX Blocks	Corrected Blocks	Uncorrected Blocks
	0	0	0	0

ADSL Status	Mode	State	Up Speed	Down Speed	SNR Margin	Loop Att.
	-----	READY	0	0	0	0

ISDN Status >> Dial ISDN >> Drop B1 >> Drop B2

Channel	Active Connection	TX Pkts	TX Rate (Bps)	RX Pkts	RX Rate (Bps)	Up Time	AOC
ISDN1-B1	Idle [---]	0	0	0	0	0:0:0	0
ISDN1-B2	Idle [---]	0	0	0	0	0:0:0	0
ISDN1-D	UP						
ISDN2-B1	2930 [192.168.3.10]	19	9	10	3	0:0:36	0
ISDN2-B2	Idle [---]	0	0	0	0	0:0:0	0
ISDN2-D	UP						

Es folgt eine detaillierte Erläuterung der Angaben:

Primär-DNS - Zeigt die IP-Adresse des bevorzugten DNS-Servers an.

Sekundär-DNS - Zeigt die IP-Adresse des alternativen DNS-Servers an.

LAN-Status

IP-Adresse - Zeigt die IP-Adresse der LAN-Schnittstelle an.

TX-Pakete - Zeigt die Gesamtanzahl der an der LAN-Schnittstelle übertragenen Pakete an.

RX-Pakete - Zeigt die Gesamtanzahl der an der LAN-Schnittstelle empfangenen Pakete an.

WAN 1-/2-Status

Anschluss - Zeigt die physische Verbindung (Ethernet) dieser Schnittstelle an.

Name - Zeigt die Bezeichnung an, die im WAN1/WAN2-Dialog festgelegt wurde.

Modus - Zeigt die Art der WAN-Verbindung an (z.B. PPPoE).

Verbindung aktiv seit - Zeigt die Gesamtbetriebszeit der Schnittstelle an.

IP - Zeigt die IP-Adresse der WAN-Schnittstelle an.

GW-IP - Zeigt die IP-Adresse des Standard-Gateways an.

TX-Pakete - Zeigt die Gesamtanzahl der an der WAN-Schnittstelle übertragenen Pakete an.

TX-Rate - Zeigt die Geschwindigkeit der an der WAN-Schnittstelle übertragenen Oktette an.

RX-Pakete - Zeigt die Gesamtanzahl der an der WAN-Schnittstelle empfangenen Pakete an.

RX-Rate - Zeigt die Geschwindigkeit der an der WAN-Schnittstelle empfangenen Oktette an.

ISDN-Status

Aktive Verbindung je Kanal - Zeigt den aktiven Verbindungsstatus für jeden Kanal an.

TX-Pakete - Zeigt die Gesamtanzahl der an der ISDN-Schnittstelle übertragenen Pakete an.

TX-Rate - Zeigt die Geschwindigkeit der an der ISDN-Schnittstelle übertragenen Oktette an.

RX-Pakete - Zeigt die Gesamtanzahl der an der ISDN-Schnittstelle empfangenen Pakete an.

RX-Rate - Zeigt die Geschwindigkeit der an der ISDN-Schnittstelle empfangenen Oktette an.

Verbindung aktiv seit - Zeigt die Gesamtbetriebszeit der Schnittstelle an.

Gebührennachweis - Zeigt die Gebühreninformation der Schnittstelle an.

Hinweis: Wird der Text in grün angezeigt, so deutet dies darauf hin, dass die WAN-Verbindung dieser Schnittstelle (WAN1/WAN2) für die Einwahl ins Internet bereit ist; wird der Text in rot angezeigt, so ist die WAN-Verbindung der Schnittstelle (WAN1/WAN2) nicht für die Einwahl ins Internet bereit.

2.4 Konfiguration speichern

Jedes Mal, wenn Sie im Dialog zur Speicherung der Konfiguration **OK** anklicken, werden Systemmeldungen angezeigt.

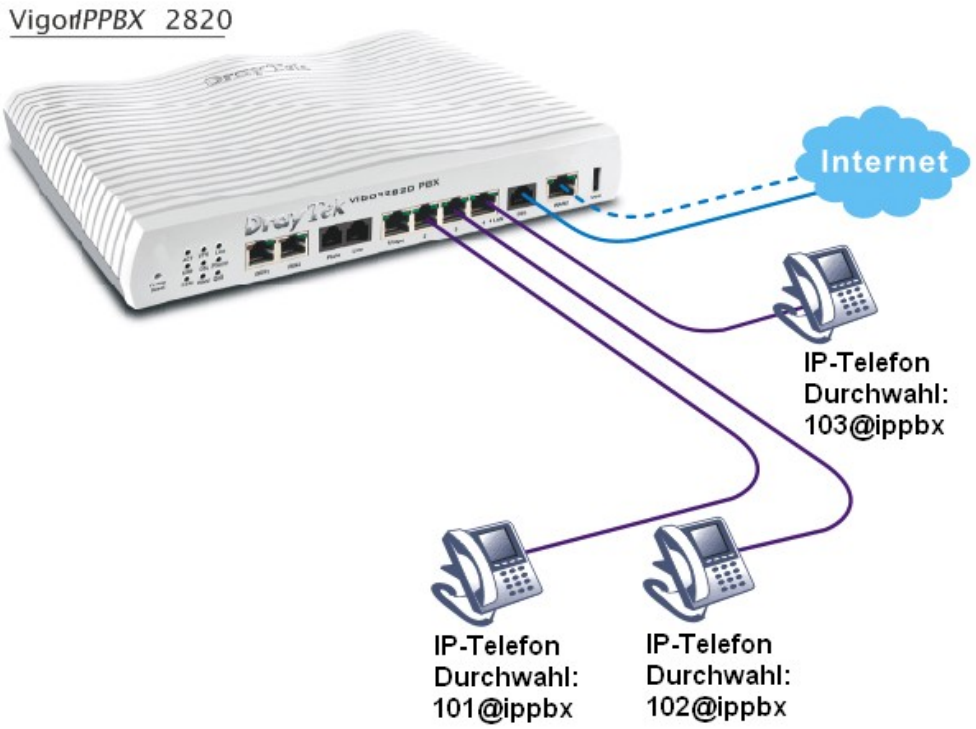
Bereit gibt an, dass das System zur Eingabe von Einstellungen bereit ist.

Einstellungen gespeichert bedeutet, dass Ihre Einstellungen gespeichert werden, sobald Sie auf **Fertigstellen** oder **OK** klicken.

Kapitel 3: Anwendungen

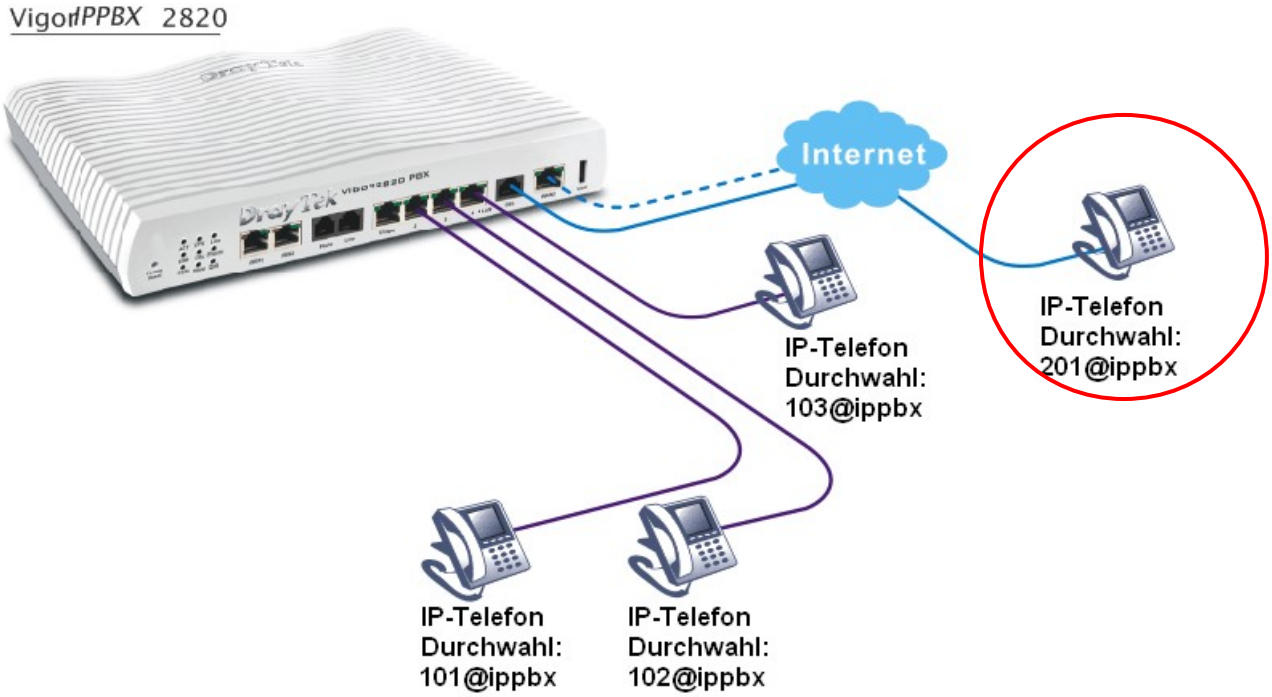
Dieses Kapitel stellt verschiedene Szenarien vor, die zeigen, wie die TK-Anlage für unterschiedliche Zwecke konfiguriert werden kann.

3.1 Anmeldung von 50 IP-basierten Telefonen/Nebenstellen



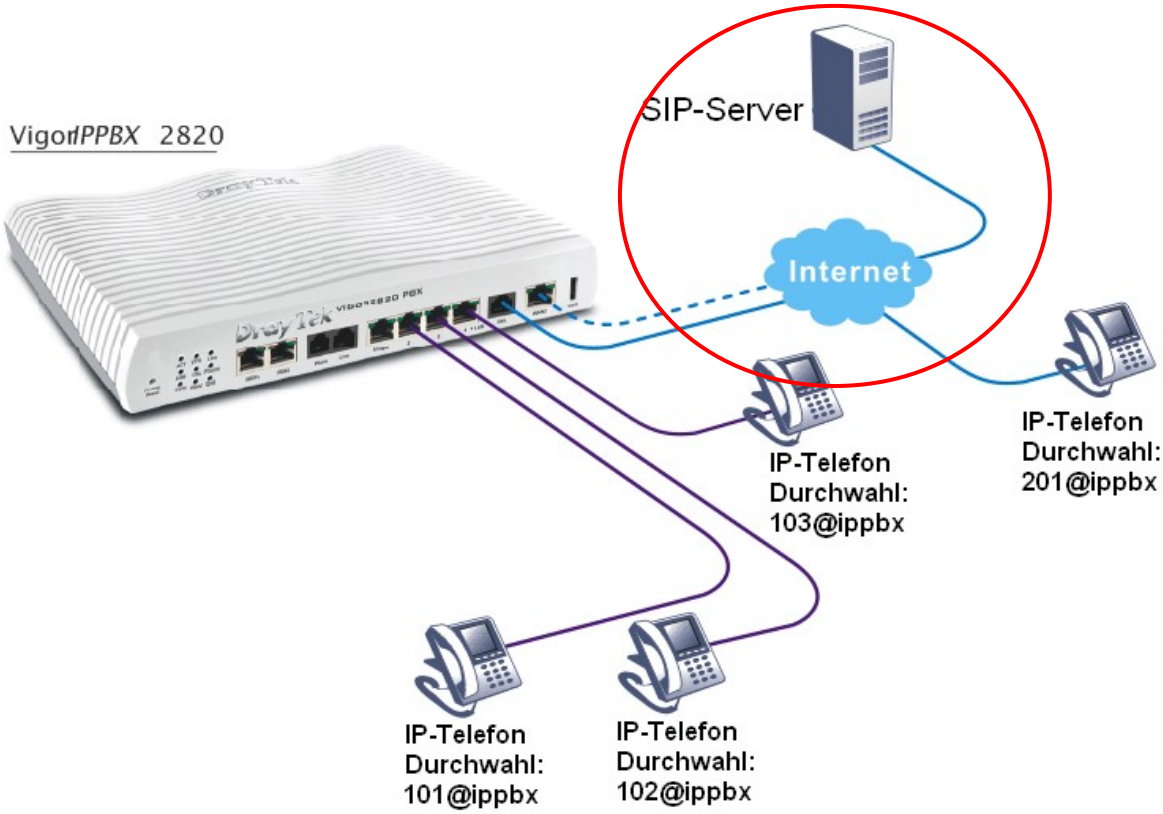
- Einwahl ins Internet über DSL.
- Flexibles zweites WAN als Backup.
- Die IP-basierten Telefone sind an den LAN-Ports angeschlossenen und als Nebenstellenrufnummern 101, 102 und 103 konfiguriert.
- Die IP-basierten Telefone (101, 102, 103) sind am Vigor*IPPBX* 2820 angemeldet.

3.2 IP-Anmeldung von entferntem Standort (über WAN-Verbindung)



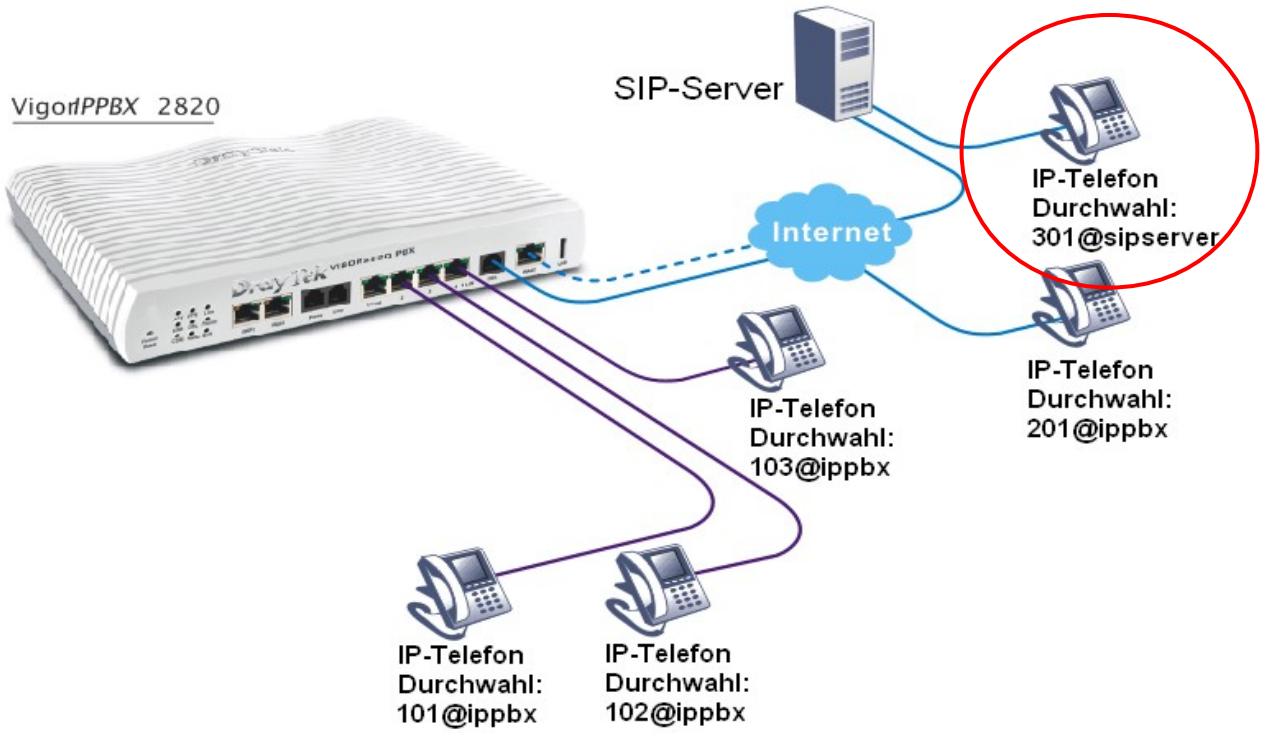
- Einwahl ins Internet über DSL.
- Flexibles zweites WAN als Backup.
- Die IP-basierten Telefone sind an den LAN-Ports angeschlossen und als Nebenstellenrufnummern 101, 102 und 103 konfiguriert.
- Die IP-basierten Telefone (101, 102, 103) und das entfernte IP-basierte Telefon sind am Vigor*IPPBX* 2820 angemeldet.
- **Das IP-basierte Telefon mit der Nebenstellenrufnummer 201 befindet sich an einem entfernten Standort.**

3.3 Integration von IP-Anmeldung über SIP-Server



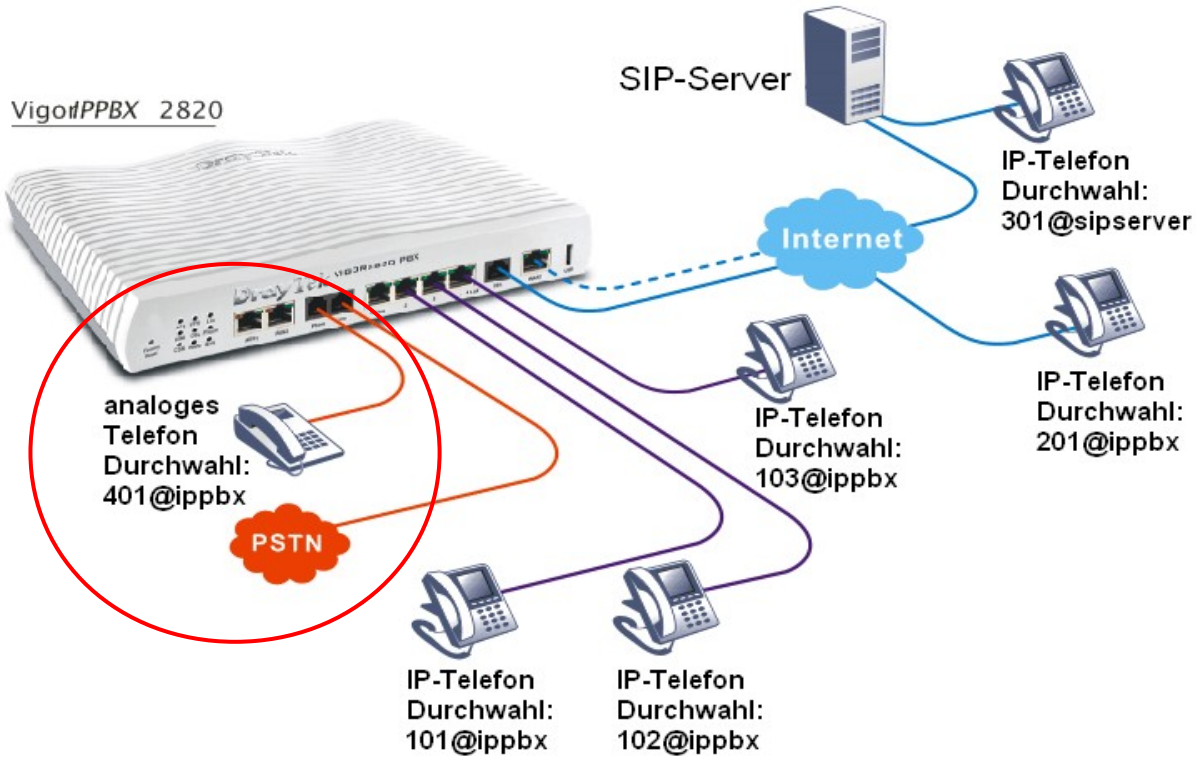
- Einwahl ins Internet über DSL.
- Flexibles zweites WAN als Backup.
- Die IP-basierten Telefone sind an den LAN-Ports angeschlossen und als Nebenstellenrufnummern 101, 102 und 103 konfiguriert.
- Die IP-basierten Telefone (101, 102, 103) und das entfernte IP-basierte Telefon sind am Vigor*IPPBX* 2820 angemeldet.
- Das IP-basierte Telefon mit der Nebenstellenrufnummer 201 befindet sich an einem entfernten Standort.
- **Der Vigor*IPPBX* 2820 kann nahtlos mit ITSP-Diensten integriert werden (ermöglicht die Anmeldung an einem SIP-Server).**

3.4 Integration von VoIP-Kommunikation über SIP-Server



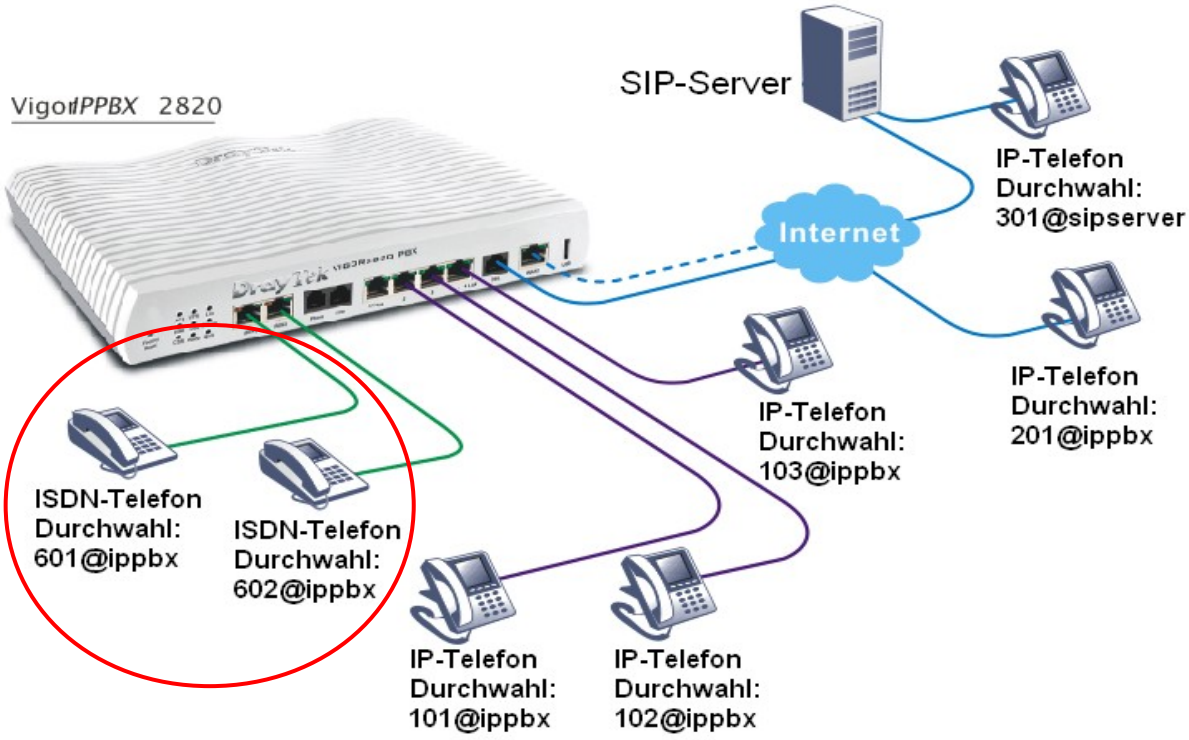
- Einwahl ins Internet über DSL.
- Flexibles zweites WAN als Backup.
- Die IP-basierten Telefone sind an den LAN-Ports angeschlossen und als Nebenstellenrufnummern 101, 102 und 103 konfiguriert.
- Die IP-basierten Telefone (101, 102, 103) und das entfernte IP-basierte Telefon sind am Vigor*IPPBX* 2820 angemeldet.
- Das IP-basierte Telefon mit der Nebenstellenrufnummer 201 befindet sich an einem entfernten Standort.
- Der Vigor*IPPBX* 2820 kann nahtlos mit ITSP-Diensten integriert werden (ermöglicht die Anmeldung an einem SIP-Server).
- **Das entfernte IP-basierte Telefon mit der Nebenstellenrufnummer 301 ist an einem SIP-Server angemeldet.**

3.5 Integration von analoger Telefonie



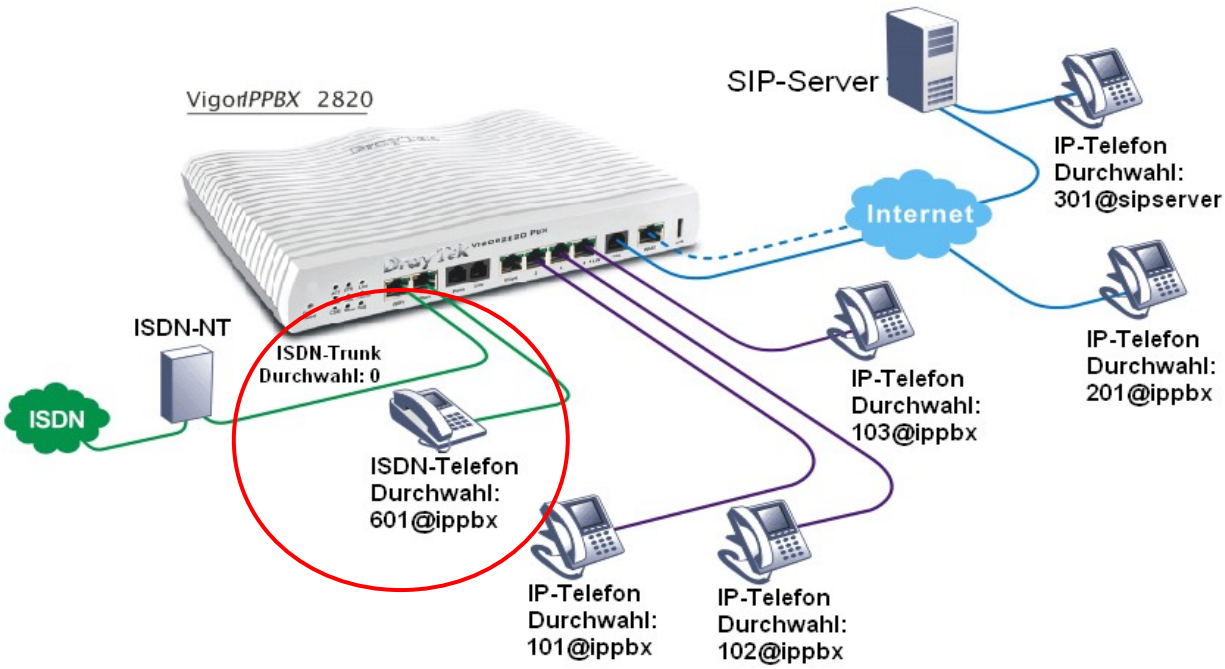
- Einwahl ins Internet über DSL.
- Flexibles zweites WAN als Backup.
- Die IP-basierten Telefone sind an den LAN-Ports angeschlossen und als Nebenstellenrufnummern 101, 102 und 103 konfiguriert.
- Die IP-basierten Telefone (101, 102, 103) und das entfernte IP-basierte Telefon sind am Vigor*IPPBX* 2820 angemeldet.
- Das IP-basierte Telefon mit der Nebenstellenrufnummer 201 befindet sich an einem entfernten Standort.
- Der Vigor*IPPBX* 2820 kann nahtlos mit ITSP-Diensten integriert werden (ermöglicht die Anmeldung an einem SIP-Server).
- Das entfernte IP-basierte Telefon mit der Nebenstellenrufnummer 301 ist an einem SIP-Server angemeldet.
- **Die analoge Amtsleitung ist am "Line"-Anschluss angeschlossen.**
- **Das analoge Telefon ist am "Phone"-Port angeschlossen und verwendet die Nebenstellenrufnummer 401 am Vigor*IPPBX* 2820.**

3.6 Zusätzliche ISDN-Telefonie



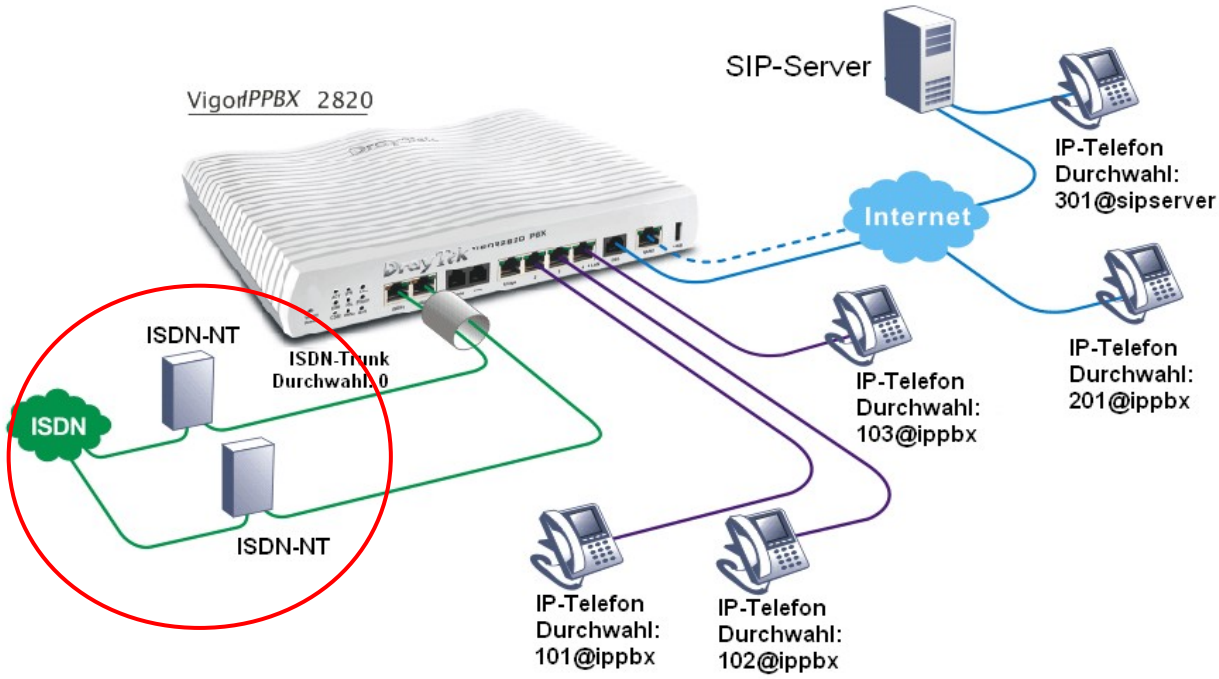
- Einwahl ins Internet über DSL.
- Flexibles zweites WAN als Backup.
- Die IP-basierten Telefone sind an den LAN-Ports angeschlossen und als Nebenstellenrufnummern 101, 102 und 103 konfiguriert.
- Die IP-basierten Telefone (101, 102, 103) und das entfernte IP-basierte Telefon sind am Vigor*IPPBX* 2820 angemeldet.
- Das IP-basierte Telefon mit der Nebenstellenrufnummer 201 befindet sich an einem entfernten Standort.
- Der Vigor*IPPBX* 2820 kann nahtlos mit ITSP-Diensten integriert werden (ermöglicht die Anmeldung an einem SIP-Server).
- Das entfernte IP-basierte Telefon mit der Nebenstellenrufnummer 301 ist an einem SIP-Server angemeldet.
- **Die ISDN-Telefone mit den Nebenstellenrufnummern 601 und 602 sind an der NT-Schnittstelle des Vigor*IPPBX* 2820 angeschlossen.**

3.7 Integrierte ISDN-Leitung



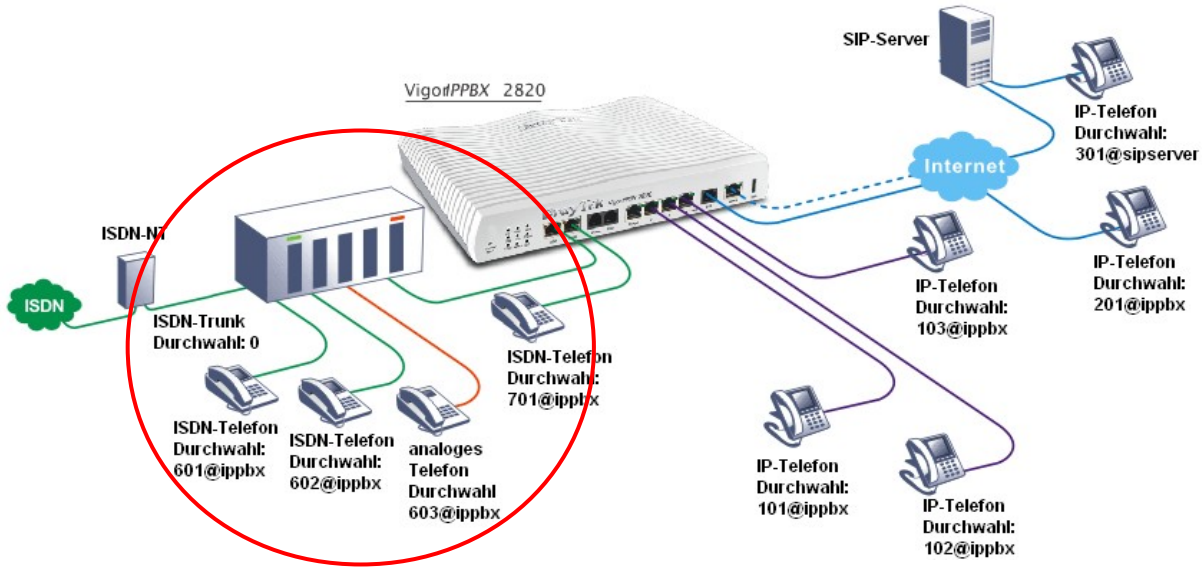
- Einwahl ins Internet über DSL.
- Flexibles zweites WAN als Backup.
- Die IP-basierten Telefone sind an den LAN-Ports angeschlossen und als Nebenstellenrufnummern 101, 102 und 103 konfiguriert.
- Die IP-basierten Telefone (101, 102, 103) und das entfernte IP-basierte Telefon sind am Vigor*IPPBX* 2820 angemeldet.
- Das IP-basierte Telefon mit der Nebenstellenrufnummer 201 befindet sich an einem entfernten Standort.
- Der Vigor*IPPBX* 2820 kann nahtlos mit ITSP-Diensten integriert werden (ermöglicht die Anmeldung an einem SIP-Server).
- Das entfernte IP-basierte Telefon mit der Nebenstellenrufnummer 301 ist an einem SIP-Server angemeldet.
- **Die ISDN-Amtsleitung ist an der TE-Schnittstelle des Vigor*IPPBX* 2820 angeschlossen.**
- **Das ISDN-Telefon mit der Nebenstellennummer 601 ist an der NT-Schnittstelle des Vigor*IPPBX* 2820 angeschlossen.**

3.8 Vier B-Kanäle der zwei ISDN-Leitungen



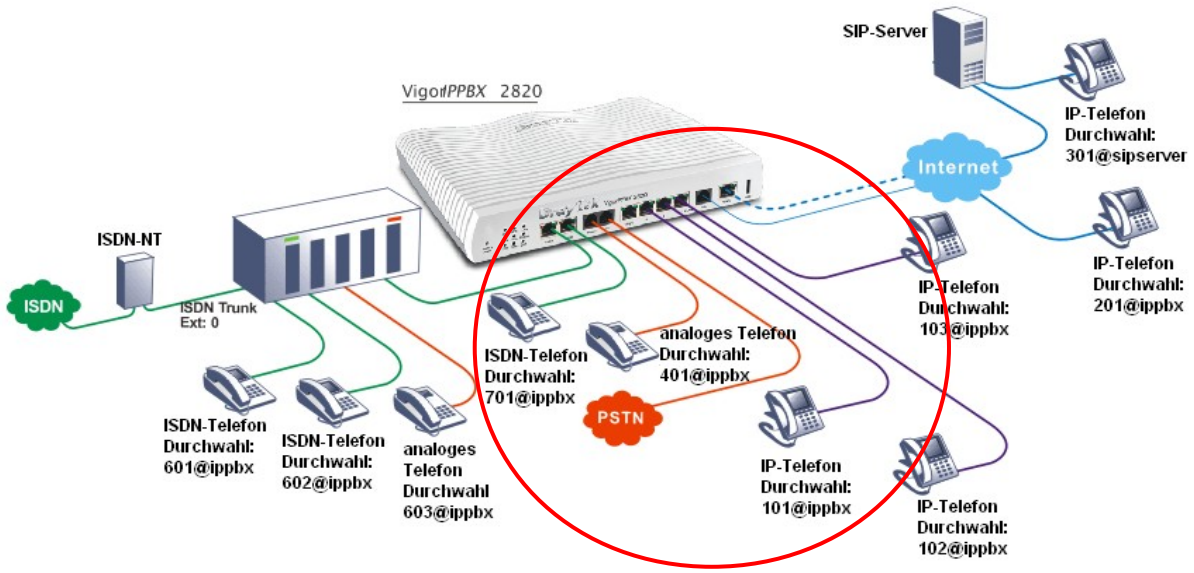
- Einwahl ins Internet über DSL.
- Flexibles zweites WAN als Backup.
- Die IP-basierten Telefone sind an den LAN-Ports angeschlossen und als Nebenstellenrufnummern 101, 102 und 103 konfiguriert.
- Die IP-basierten Telefone (101, 102, 103) und das entfernte IP-basierte Telefon sind am Vigor*IPPBX* 2820 angemeldet.
- Das IP-basierte Telefon mit der Nebenstellenrufnummer 201 befindet sich an einem entfernten Standort.
- Der Vigor*IPPBX* 2820 kann nahtlos mit ITSP-Diensten integriert werden (ermöglicht die Anmeldung an einem SIP-Server).
- Das entfernte IP-basierte Telefon mit der Nebenstellenrufnummer 301 ist an einem SIP-Server angemeldet.
- **Die zwei ISDN-Leitungen sind an zwei TE-Schnittstellen am *VigorIPPBX* 2820 angeschlossen.**

3.9 Integration einer ISDN-TK-Anlage mit einer ISDN-Leitung



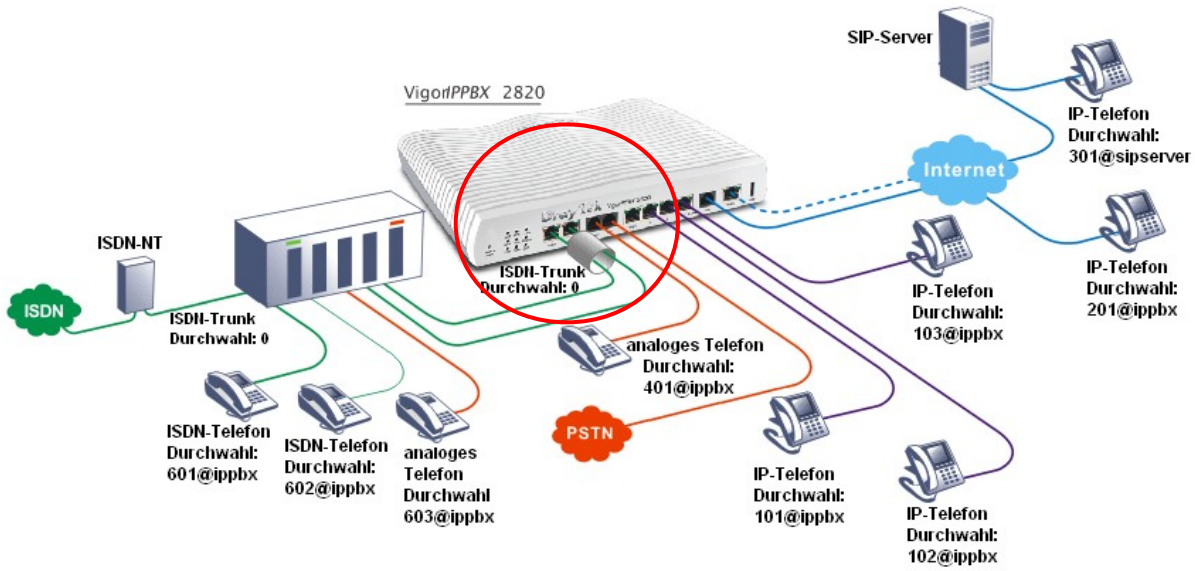
- Einwahl ins Internet über DSL.
- Flexibles zweites WAN als Backup.
- Die IP-basierten Telefone sind an den LAN-Ports angeschlossen und als Nebenstellenrufnummern 101, 102 und 103 konfiguriert.
- Die IP-basierten Telefone (101, 102, 103) und das entfernte IP-basierte Telefon sind am Vigor*IPPBX* 2820 angemeldet.
- Das IP-basierte Telefon mit der Nebenstellenrufnummer 201 befindet sich an einem entfernten Standort.
- Der Vigor*IPPBX* 2820 kann nahtlos mit ITSP-Diensten integriert werden (ermöglicht die Anmeldung an einem SIP-Server).
- Das entfernte IP-basierte Telefon mit der Nebenstellenrufnummer 301 ist an einem SIP-Server angemeldet.
- **Das ISDN-Telefon mit der Nebenstellennummer 701 ist an der NT-Schnittstelle des Vigor*IPPBX* 2820 angeschlossen.**
- **Die ISDN-TK-Anlage ist an der TE-Schnittstelle des Vigor*IPPBX* 2820 angeschlossen. Die ISDN-Telefone mit den Nebenstellenrufnummern 601 und 602 sind an der ISDN-TK-Anlage angeschlossen.**
- **Die ISDN-TK-Anlage bietet auch die Möglichkeit, analoge Telefone anzuschließen. Das analoge Telefon mit der Nebenstellenrufnummer 601 ist an der ISDN-TK-Anlage angeschlossen.**

3.10 Netzwerkaufbau (ISDN und analog)



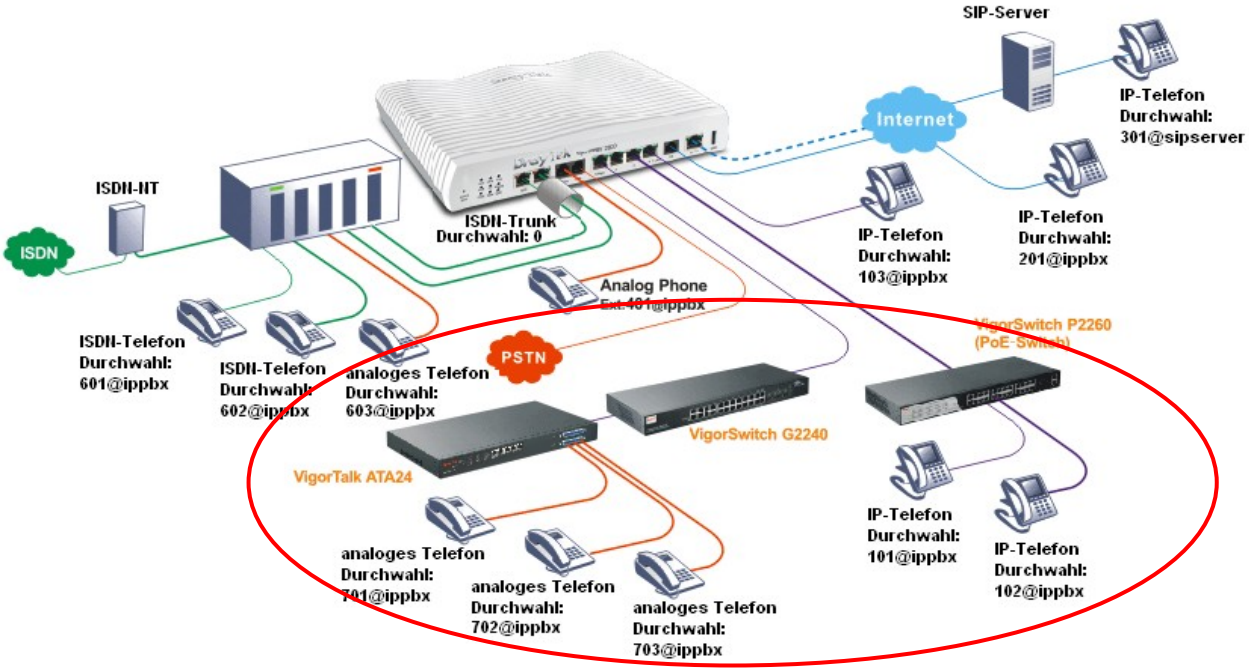
- Einwahl ins Internet über DSL.
- Flexibles zweites WAN als Backup.
- Die IP-basierten Telefone sind an den LAN-Ports angeschlossen und als Nebenstellenrufnummern 101, 102 und 103 konfiguriert.
- Die IP-basierten Telefone (101, 102, 103) und das entfernte IP-basierte Telefon sind am Vigor*IPPBX* 2820 angemeldet.
- Das IP-basierte Telefon mit der Nebenstellenrufnummer 201 befindet sich an einem entfernten Standort.
- Der Vigor*IPPBX* 2820 kann nahtlos mit ITSP-Diensten integriert werden (ermöglicht die Anmeldung an einem SIP-Server).
- Das entfernte IP-basierte Telefon mit der Nebenstellenrufnummer 301 ist an einem SIP-Server angemeldet.
- Das ISDN-Telefon mit der Nebenstellennummer 701 ist an der NT-Schnittstelle des Vigor*IPPBX* 2820 angeschlossen.
- Die ISDN-TK-Anlage ist an der TE-Schnittstelle des Vigor*IPPBX* 2820 angeschlossen. Die ISDN-Telefone mit den Nebenstellenrufnummern 601 und 602 sind an der ISDN-TK-Anlage angeschlossen.
- Die ISDN-TK-Anlage bietet auch die Möglichkeit, analoge Telefone anzuschließen. Das analoge Telefon mit der Nebenstellenrufnummer 601 ist an der ISDN-TK-Anlage angeschlossen.
- **Die analoge Amtsleitung ist am "Line"-Anschluss angeschlossen.**
- **Das analoge Telefon ist am "Phone"-Port angeschlossen und verwendet die Nebenstellenrufnummer 401 am Vigor*IPPBX* 2820.**

3.11 Integration von ISDN-Telefonie und analogem Netzwerk



- Einwahl ins Internet über DSL.
- Flexibles zweites WAN als Backup.
- Die IP-basierten Telefone sind an den LAN-Ports angeschlossen und als Nebenstellenrufnummern 101, 102 und 103 konfiguriert.
- Die IP-basierten Telefone (101, 102, 103) und das entfernte IP-basierte Telefon sind am Vigor*IPPBX* 2820 angemeldet.
- Das IP-basierte Telefon mit der Nebenstellenrufnummer 201 befindet sich an einem entfernten Standort.
- Der Vigor*IPPBX* 2820 kann nahtlos mit ITSP-Diensten integriert werden (ermöglicht die Anmeldung an einem SIP-Server).
- Das entfernte IP-basierte Telefon mit der Nebenstellenrufnummer 301 ist an einem SIP-Server angemeldet.
- Die ISDN-Telefone mit den Nebenstellenrufnummern 601 und 602 sind an der ISDN-TK-Anlage angeschlossen.
- Die ISDN-TK-Anlage bietet auch die Möglichkeit, analoge Telefone anzuschließen. Das analoge Telefon mit der Nebenstellenrufnummer 601 ist an der ISDN-TK-Anlage angeschlossen.
- Die analoge Amtsleitung ist am "Line"-Anschluss angeschlossen.
- Das analoge Telefon ist am "Phone"-Port angeschlossen und verwendet die Nebenstellenrufnummer 401 am Vigor*IPPBX* 2820.
- **Die zwei internen Leitungen der ISDN-TK-Anlage sind an den TE-Schnittstellen des Vigor*IPPBX* 2820 angeschlossen.**

3.12 Integration von ISDN-Telefonie, analogem Netzwerk und VoIP-Verbindung

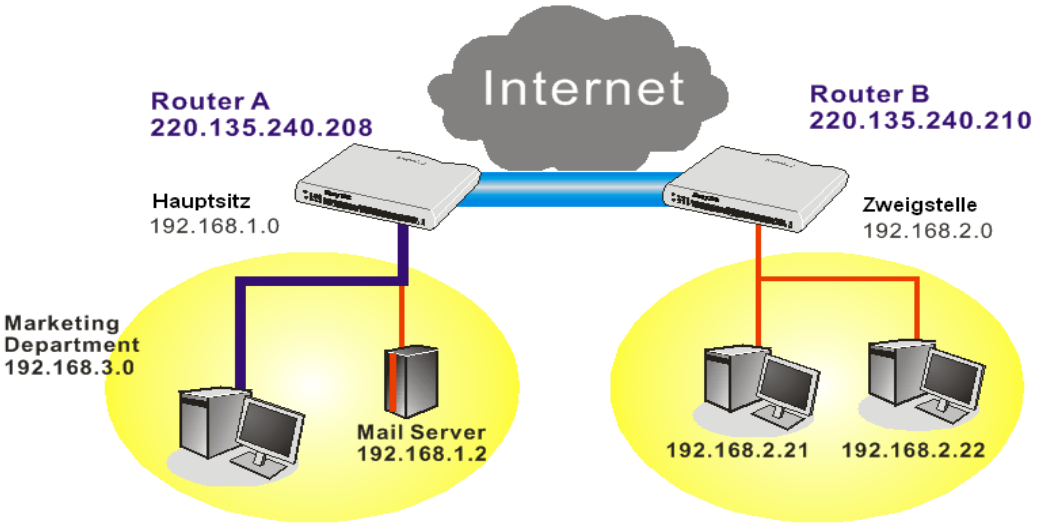


- Einwahl ins Internet über DSL.
- Flexibles zweites WAN als Backup.
- Die IP-basierten Telefone mit den Nebenstellenrufnummern 101 und 102 sind an den LAN-Ports des **VigorSwitch** angeschlossen. **Die analogen Telefone mit den Nebenstellenrufnummern 701, 702 und 703 sind am VigorTalk ATA24 angeschlossen und am Vigor*IPPBX 2820* angemeldet.**
- Das IP-basierte Telefon mit der Nebenstellenrufnummer 103 und das entfernte IP-basierte Telefon mit der Nebenstellenrufnummer 201 sind angemeldet.
- Das IP-basierte Telefon mit der Nebenstellenrufnummer 201 befindet sich an einem entfernten Standort.
- Der Vigor*IPPBX* 2820 kann nahtlos mit ITSP-Diensten integriert werden (ermöglicht die Anmeldung an einem SIP-Server).
- Das entfernte IP-basierte Telefon mit der Nebenstellenrufnummer 301 ist an einem SIP-Server angemeldet.
- Die ISDN-Telefone mit den Nebenstellenrufnummern 601 und 602 sind an der ISDN-TK-Anlage angeschlossen.
- Über die ISDN-TK-Anlage können auch analoge Telefone angeschlossen werden. Das Telefon mit Nebenstellenrufnummer 601 ist an der ISDN-TK-Anlage angeschlossen.
- Die analoge Amtsleitung ist am "Line"-Anschluss angeschlossen.
- Das analoge Telefon ist am "Phone"-Port angeschlossen und verwendet die Nebenstellenrufnummer 401 am Vigor*IPPBX* 2820.
- Die zwei internen Leitungen der ISDN-TK-Anlage sind an den TE-Schnittstellen des Vigor*IPPBX* 2820 angeschlossen.

Kapitel 4: Weitere Anwendungen

4.1 LAN-zu-LAN-Verbindung zwischen Filiale und Zentrale einrichten

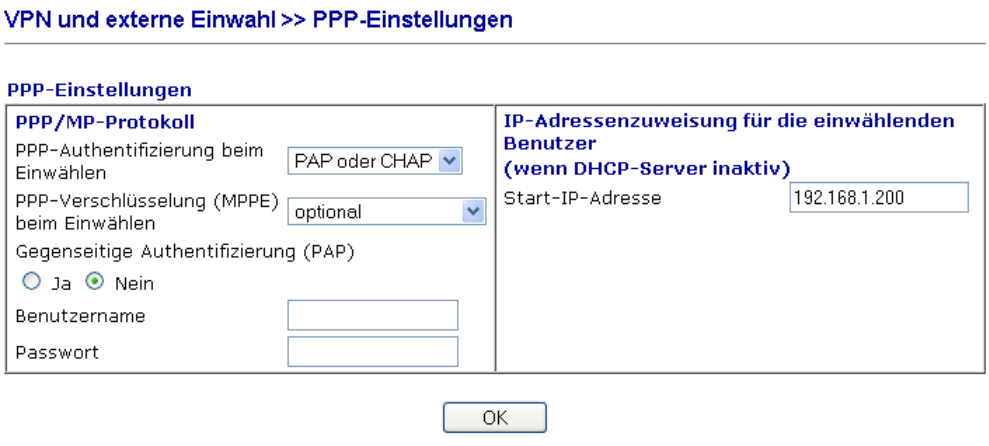
Das häufigste Szenario besteht darin, dass Sie eine sichere Netzwerkverbindung einrichten möchten, beispielsweise zwischen einer Filiale und der Zentrale. Um die abgebildete Netzwerkstruktur einzurichten, befolgen Sie die folgenden Schritte und erstellen ein LAN-zu-LAN-Profil. Diese beiden Netzwerke (LANs) sollten NICHT die gleiche Netzwerkadresse haben.



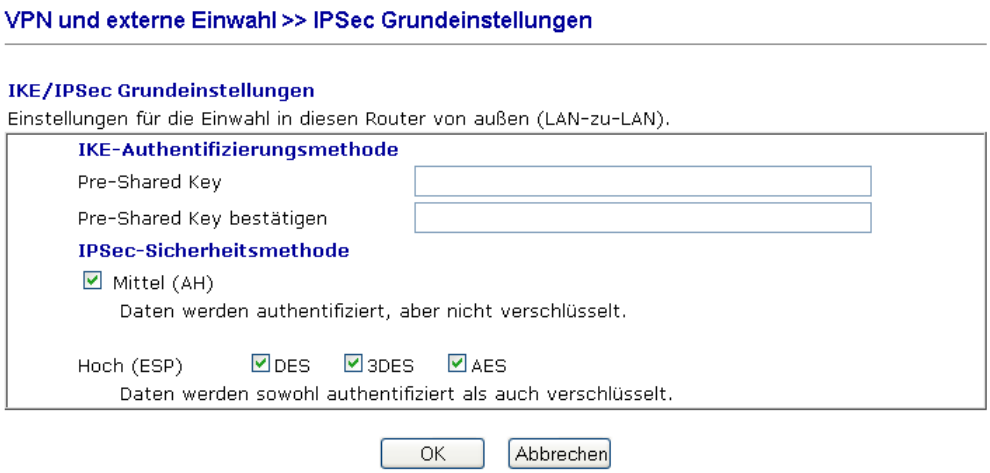
Einstellungen auf Router A in der Zentrale:

1. Gehen Sie zu **VPN und externe Einwahl**, wählen Sie **Einwahlmöglichkeiten**, um den erforderlichen VPN-Dienst zu ermöglichen, und klicken Sie auf **OK**.

2. Um **PPP**-basierte Dienste wie PPTP oder L2TP zu verwenden, konfigurieren Sie die allgemeinen Einstellungen unter **PPP-Einstellungen**.

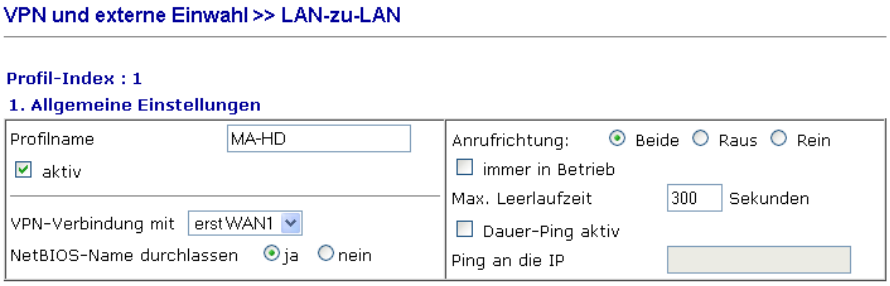


Um **IPSec**-basierte Dienste wie IPSec oder L2TP mit IPSec zu verwenden, konfigurieren Sie die Einstellungen in **IPSec-Grundeinstellungen**, z.B. den Pre-Shared Key, den beide Seiten kennen.

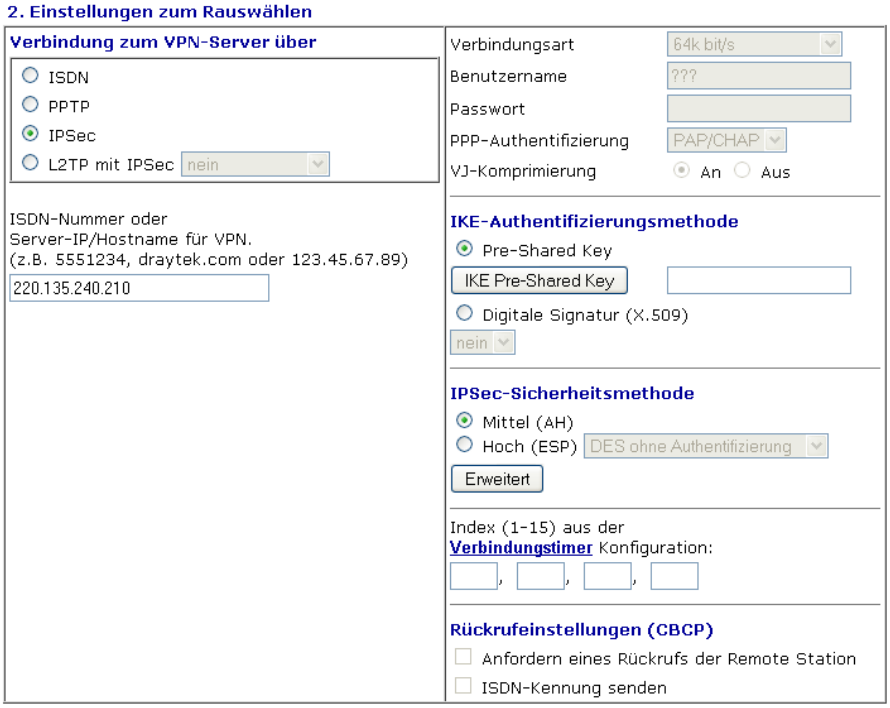


3. Gehen Sie zu **LAN zu LAN**. Klicken Sie auf eine der Indexnummern, um ein Profil zu bearbeiten.

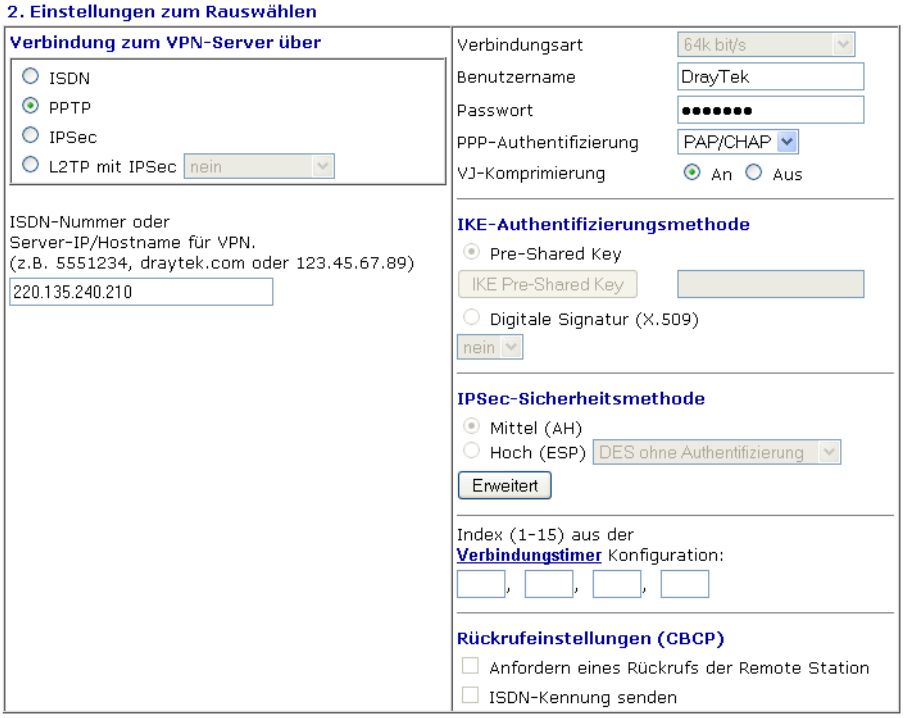
4. Konfigurieren Sie die **Allgemeinen Einstellungen** wie unten gezeigt. Aktivieren Sie beide VPN-Verbindungen, damit jede Partei die VPN-Verbindung starten kann.



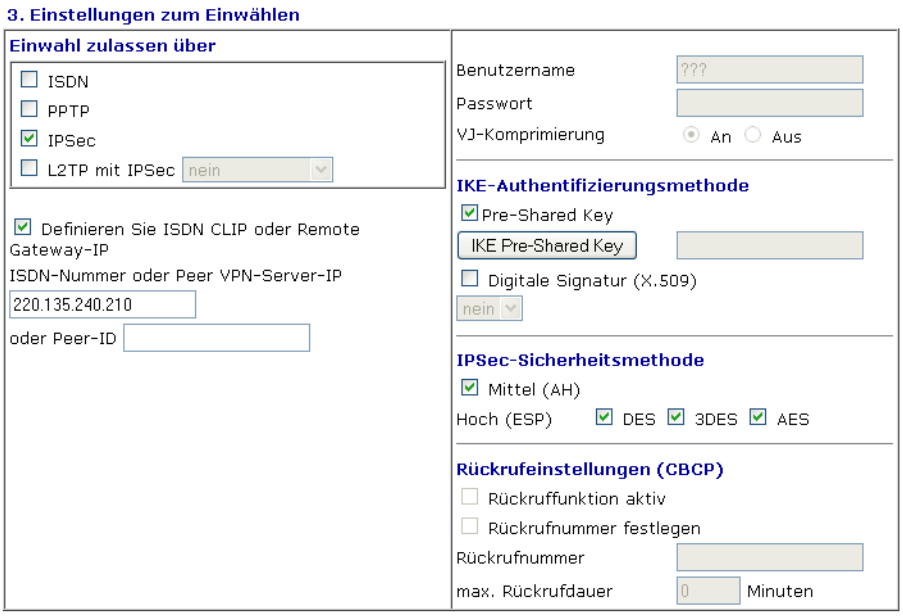
Konfigurieren Sie die **Einstellungen zum Rauswählen** wie unten gezeigt, um den Router B über die gewählte Anwahlmethode aggressiv anzuwählen.
Bei Auswahl eines ***IPSec-basierten*** Dienstes müssen Sie außerdem die IP-Adresse des entfernten Peers, die IKE-Authentifizierungsmethode und die IPSec-Verschlüsselungsmethode für diese Anwahlverbindung angeben.



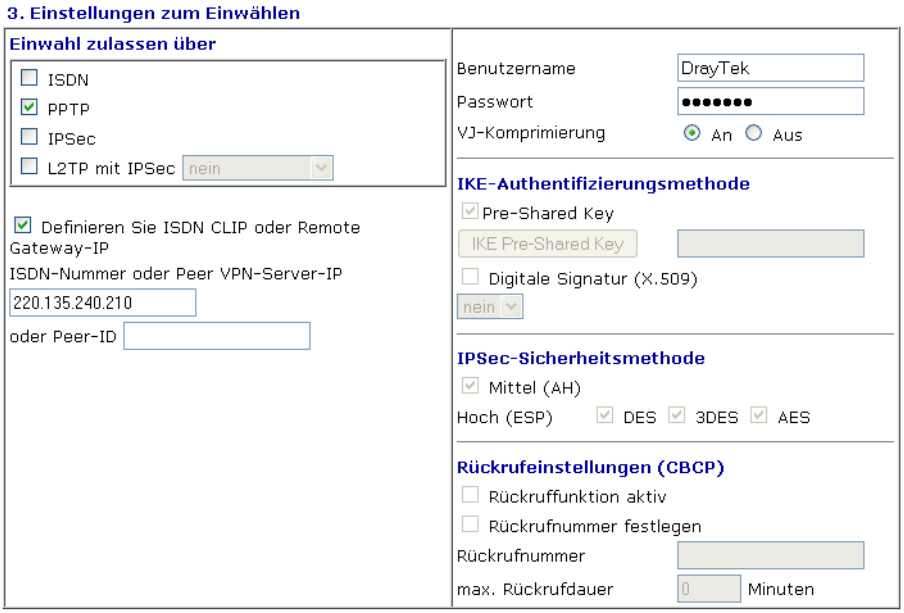
Bei Auswahl eines ***PPP-basierten Dienstes*** müssen Sie außerdem die IP-Adresse des entfernten Peers, den Benutzernamen, das Passwort, PPP-Authentifizierung und VJ-Komprimierung für diese Anwahlverbindung angeben.



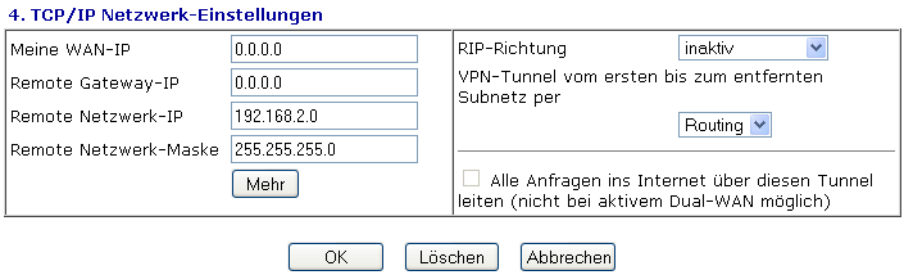
5. Konfigurieren Sie die **Einstellungen zum Einwählen** wie unten abgebildet, um Router B die Einwahl zum Aufbau einer VPN-Verbindung zu ermöglichen.Bei Auswahl eines ***IPSec-basierten*** Dienstes können Sie außerdem die IP-Adresse des entfernten Peers, die IKE-Authentifizierungsmethode und die IPSec-Verschlüsselungsmethode für diese Einwahlverbindung angeben. Ansonsten werden die obigen **IPSec Grundeinstellungen** verwendet.



Bei Auswahl eines ***PPP-basierten Dienstes*** müssen Sie außerdem die IP-Adresse des entfernten Peers, den Benutzernamen, das Passwort und VJ-Komprimierung für diese Einwahlverbindung angeben.



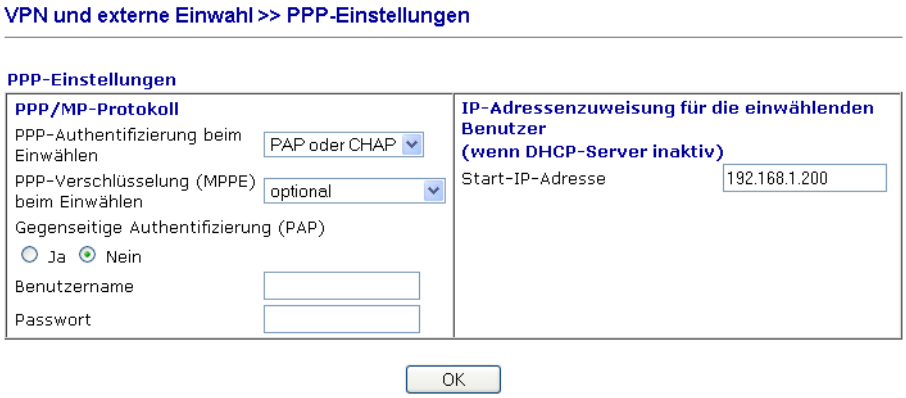
6. Schließlich konfigurieren Sie die entfernte Netzwerk-IP/das entfernte Subnetz in **TCP/IP-Netzwerkeinstellungen** so, dass der Router A die an Router B im entfernten Netzwerk bestimmten Pakete über die VPN-Verbindung übertragen kann.



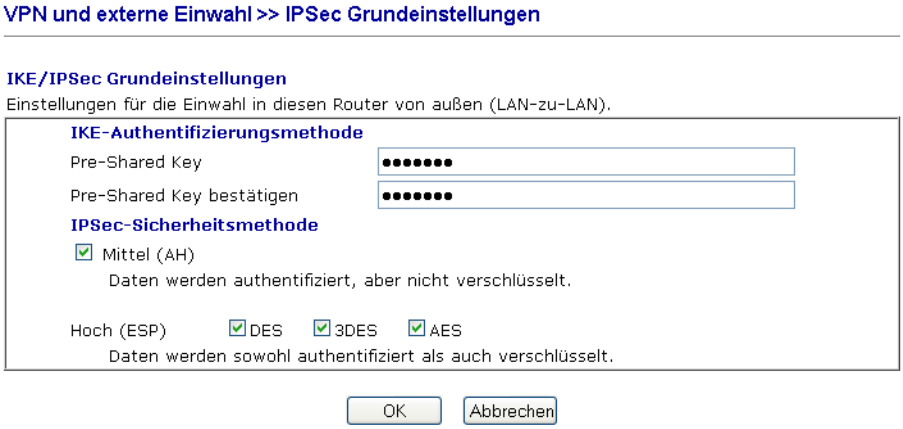
Einstellungen auf dem Router B im entfernten Büro:

1. Gehen Sie zu **VPN und externe Einwahl**, wählen Sie **Einwahlmöglichkeiten**, um den erforderlichen VPN-Dienst zu ermöglichen, und klicken Sie auf **OK**.

2. Um **PPP**-basierte Dienste wie PPTP oder L2TP zu verwenden, konfigurieren Sie die allgemeinen Einstellungen unter **PPP-Einstellungen**.

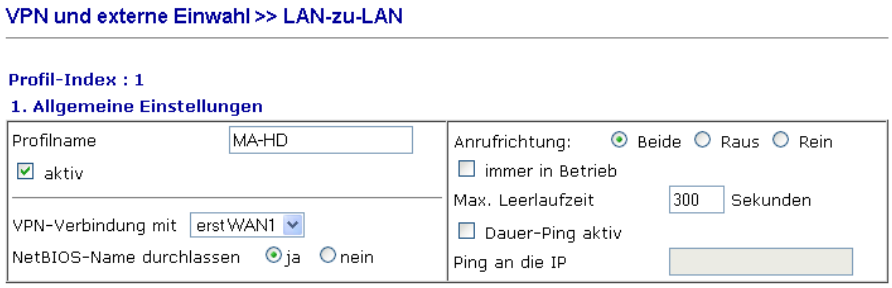


Um **IPSec**-basierte Dienste wie IPSec oder L2TP mit IPSec zu verwenden, konfigurieren Sie die Einstellungen in **IPSec-Grundeinstellungen**, z.B. den Pre-Shared Key, den beide Seiten kennen.



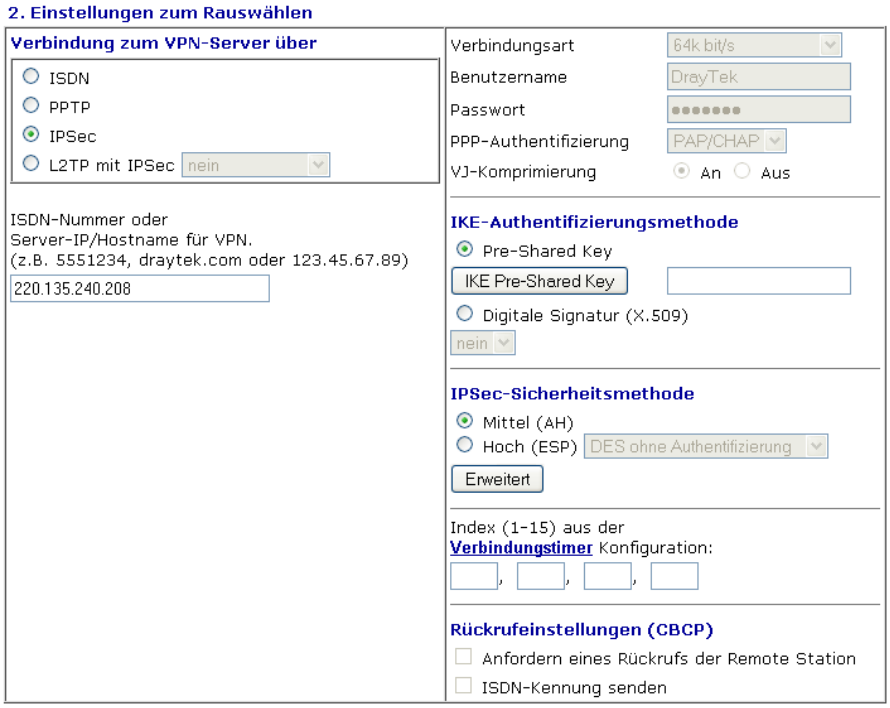
3. Gehen Sie zu **LAN zu LAN**. Klicken Sie auf eine der Indexnummern, um ein Profil zu bearbeiten.

4. Konfigurieren Sie die **Allgemeinen Einstellungen** wie unten gezeigt. Aktivieren Sie beide VPN-Verbindungen, damit jede Partei die VPN-Verbindung starten kann.

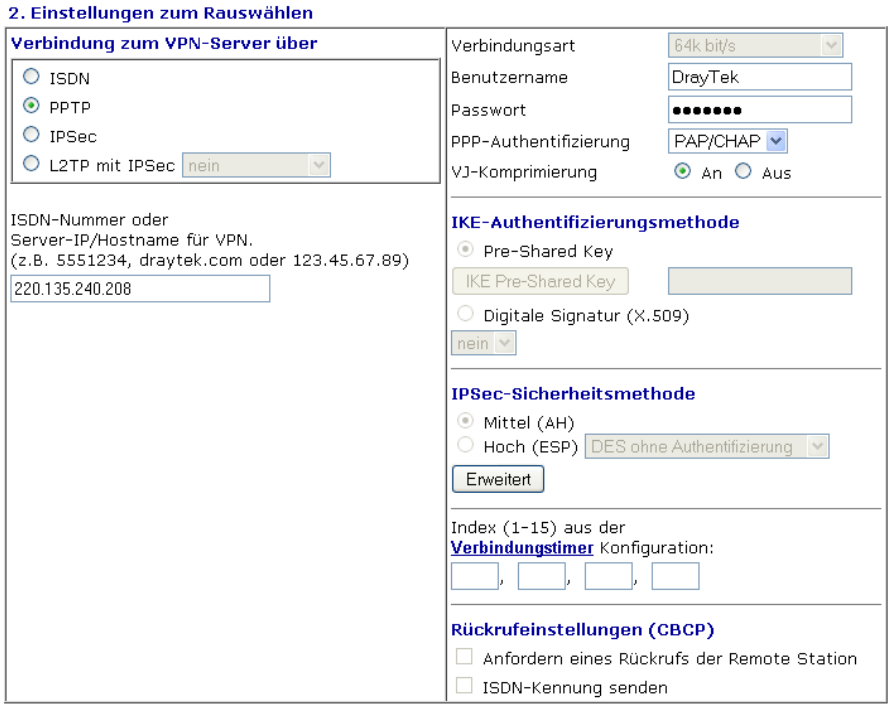


5. Konfigurieren Sie die **Einstellungen zum Rauswählen** wie unten gezeigt, um den Router B über die gewählte Anwahlmethode aggressiv anzuwählen.

Bei Auswahl eines ***IPSec-basierten*** Dienstes müssen Sie außerdem die IP-Adresse des entfernten Peers, die IKE-Authentifizierungsmethode und die IPSec-Verschlüsselungsmethode für diese Anwahlverbindung angeben.



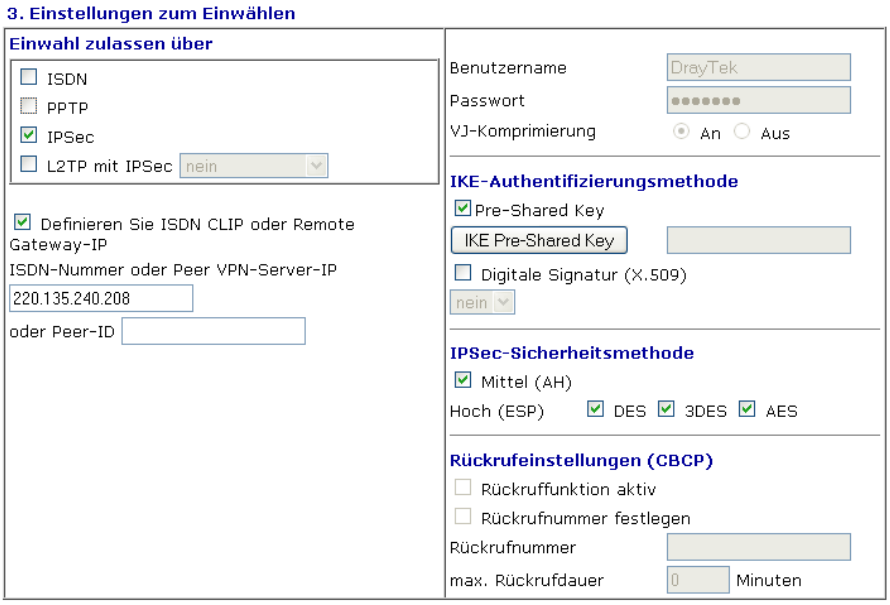
Bei Auswahl eines ***PPP-basierten Dienstes*** müssen Sie außerdem die IP-Adresse des entfernten Peers, den Benutzernamen, das Passwort, PPP-Authentifizierung und VJ-Komprimierung für diese Anwahlverbindung angeben.



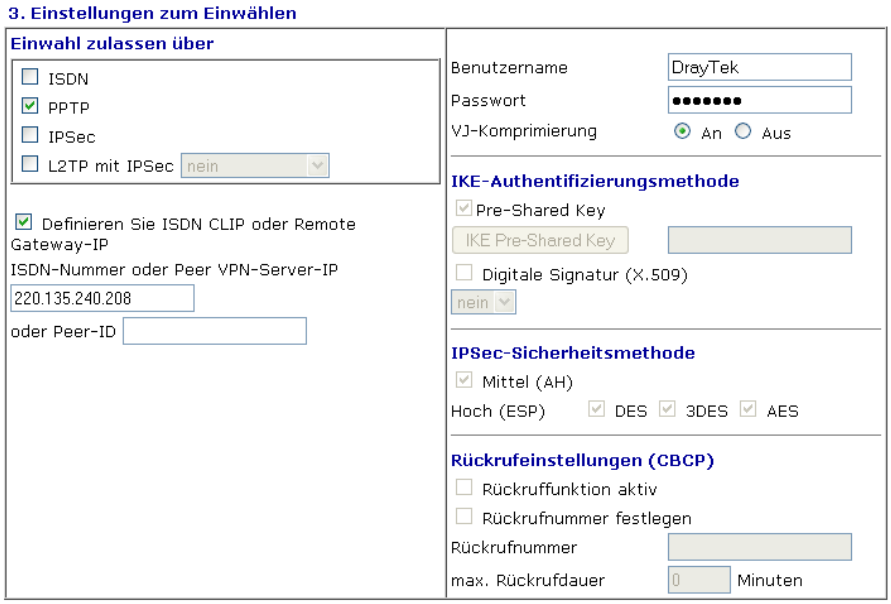
6. Konfigurieren Sie die **Einstellungen zum Einwählen** wie unten abgebildet, um Router A die Einwahl zum Aufbau einer VPN-Verbindung zu ermöglichen.

Bei Auswahl eines ***IPSec-basierten*** Dienstes können Sie außerdem die IP-Adresse des entfernten Peers, die IKE-Authentifizierungsmethode und die IPSec-Verschlüsselungsmethode für diese Einwahlverbindung angeben. Ansonsten

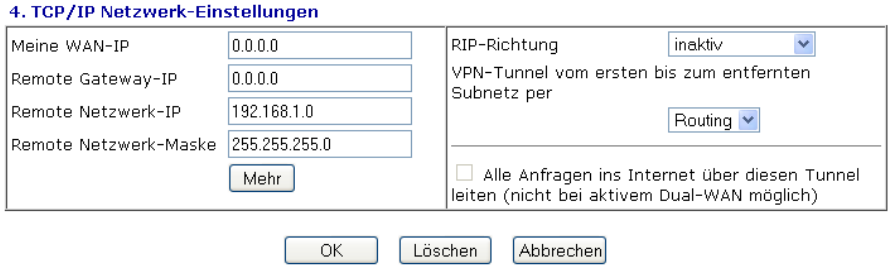
werden die obigen **IPSec Grundeinstellungen** verwendet.



Bei Auswahl eines ***PPP-basierten Dienstes*** müssen Sie außerdem die IP-Adresse des entfernten Peers, den Benutzernamen, das Passwort und VJ-Komprimierung für diese Einwahlverbindung angeben.

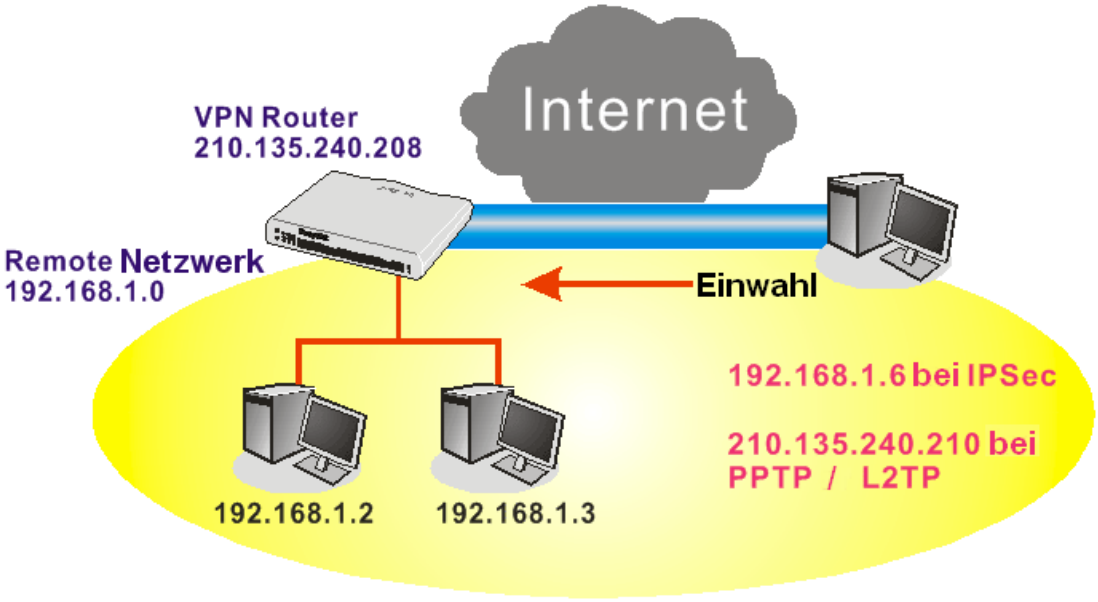


7. Schließlich konfigurieren Sie die entfernte Netzwerk-IP/das entfernte Subnetz in **TCP/IP-Netzwerkeinstellungen** so, dass der Router B die an Router A im entfernten Netzwerk bestimmten Pakete über die VPN-Verbindung übertragen kann.



4.2 Einwahlverbindung zwischen externem Teleworker und Zentrale einrichten

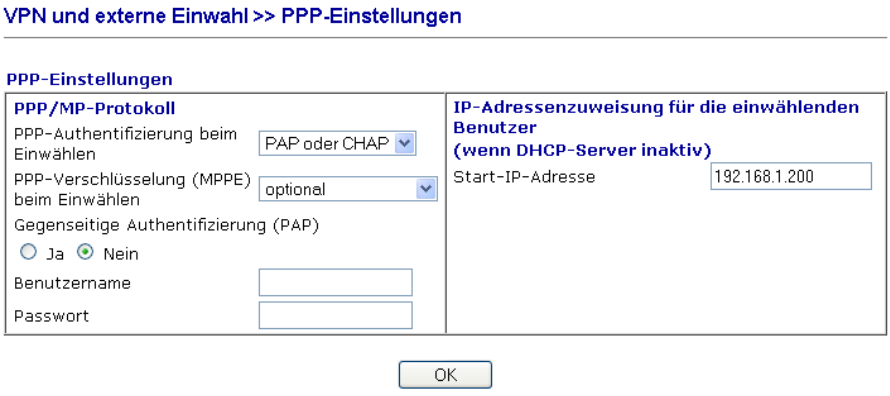
Ein anderes verbreitetes Szenario: Ein Teleworker möchte eine sichere Verbindung zum Unternehmensnetzwerk aufbauen. Um die abgebildete Netzwerkstruktur einzurichten, erstellen Sie ein Fernbenutzerprofil und installieren einen Smart VPN Client auf dem entfernten Host.



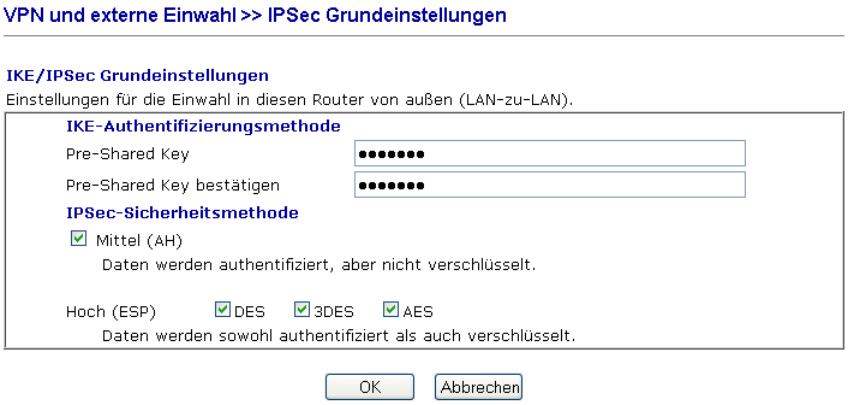
Einstellungen auf dem VPN-Router im Unternehmensbüro:

1. Gehen Sie zu **VPN und externe Einwahl**, wählen Sie **Einwahlmöglichkeiten**, um den erforderlichen VPN-Dienst zu ermöglichen, und klicken Sie auf **OK**.

2. Um PPP-basierte Dienste wie PPTP oder L2TP zu verwenden, konfigurieren Sie die allgemeinen Einstellungen unter **PPP-Einstellungen**.



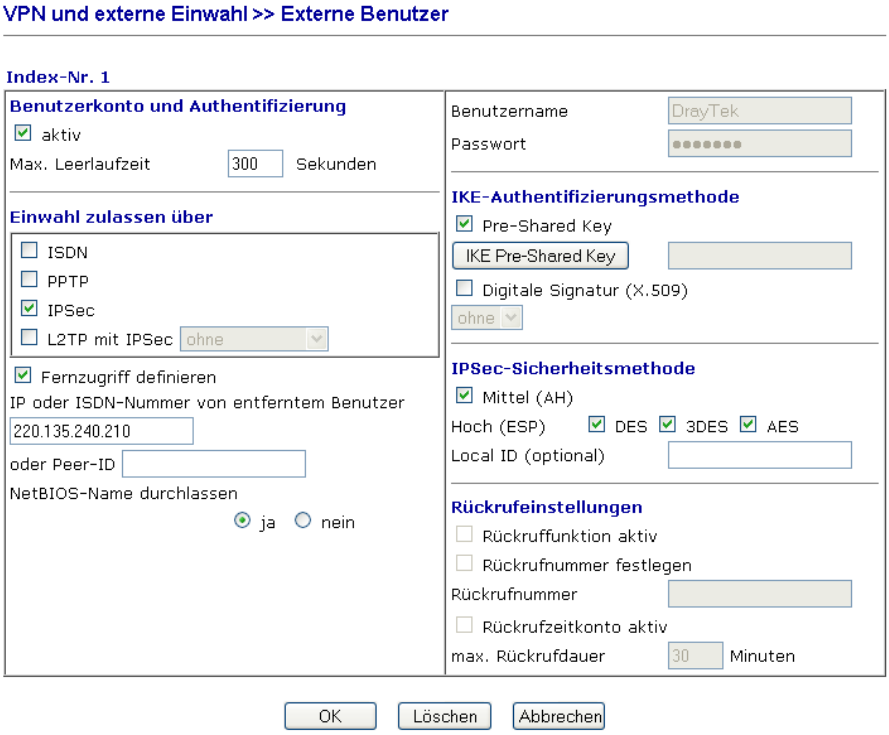
Um IPSec-basierte Dienste wie IPSec oder L2TP mit IPSec zu verwenden, konfigurieren Sie die Einstellungen in **IKE/IPSec-Grundeinstellungen**, z.B. den Pre-Shared Key, den beide Seiten kennen.



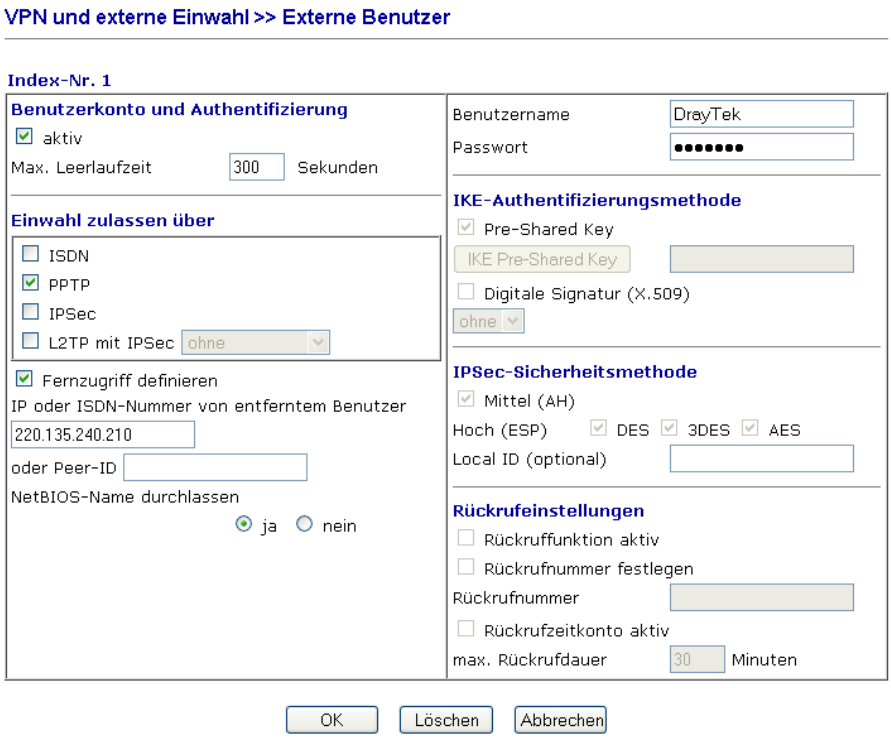
3. Gehen Sie zu **Externe Benutzer**. Klicken Sie auf eine der Indexnummern, um ein Profil zu bearbeiten.

4. Konfigurieren Sie die **Einstellungen zum Einwählen** wie unten angezeigt, um den entfernten Benutzer die Einwahl zum Aufbau einer VPN-Verbindung zu ermöglichen.

Bei Auswahl eines ***IPSec-basierten*** Dienstes können Sie außerdem die IP-Adresse des entfernten Peers, die IKE-Authentifizierungsmethode und die IPSec-Verschlüsselungsmethode für diese Einwahlverbindung angeben. Ansonsten werden die obigen **IPSec Grundeinstellungen** verwendet.



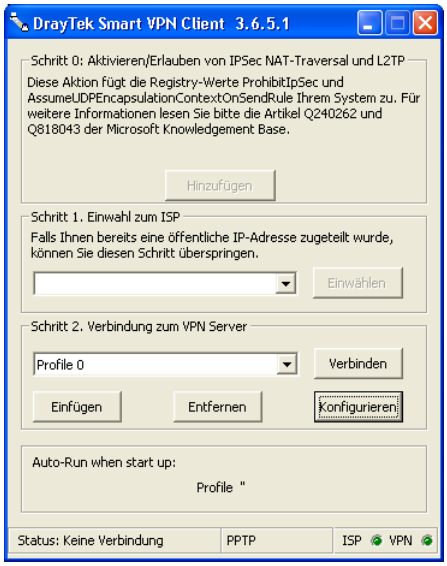
Bei Auswahl eines ***PPP-basierten*** Dienstes müssen Sie außerdem die IP-Adresse des entfernten Peers, den Benutzernamen, das Passwort und VJ-Komprimierung für diese Einwahlverbindung angeben.



Einstellungen auf dem entfernten Host:

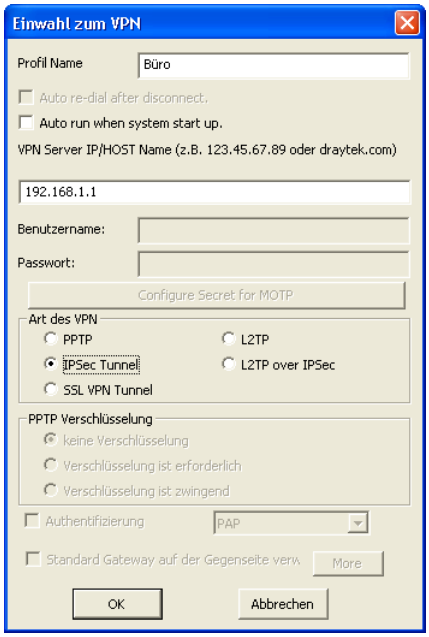
1. In Win98/ME können Sie "DFÜ-Netzwerk" verwenden, um einen PPTP-Tunnel zum Vigor-Router aufzubauen. In Win2000/XP verwenden Sie bitte die "Netzwerk- und Internetverbindungen" oder das kostenlose Programm "Smart VPN Client", um einen PPTP, L2TP bzw. L2TP über IPSec Tunnel aufzubauen. Dieses Programm kann von der beigefügten CD-ROM installiert werden oder von www.draytek.de heruntergeladen werden. Führen Sie die Installation gemäß den Anweisungen durch.

2. Nach erfolgreicher Installation sollten Sie bei erstmaliger Benutzung das **Profil 0** einstellen. Klicken Sie dann auf **Konfigurieren**. Starten Sie den Host neu.

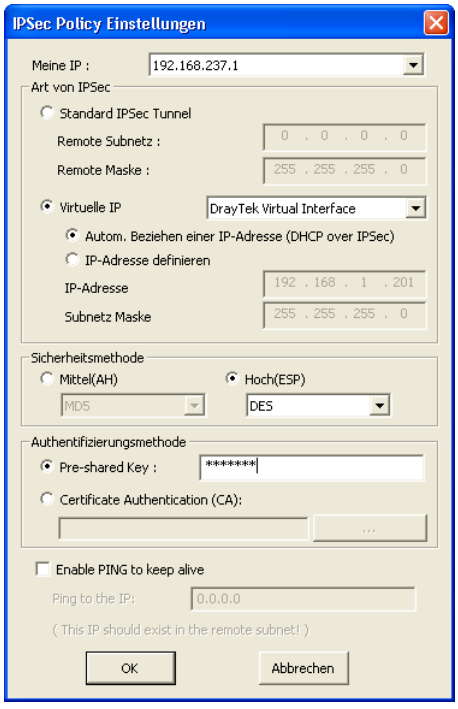

DrayTek Smart VPN Client 3.6.5.1
Schritt 0: Aktivieren/Erlauben von IPSec NAT-Traversal und L2TP
Diese Aktion fügt die Registry-Werte ProhibitIpSec und AssumeUDPEncapsulationContextOnSendRule Ihrem System zu. Für weitere Informationen lesen Sie bitte die Artikel Q240262 und Q818043 der Microsoft Knowledgement Base.
Hinzufügen
Schritt 1. Einwahl zum ISP
Falls Ihnen bereits eine öffentliche IP-Adresse zugeteilt wurde, können Sie diesen Schritt überspringen.
Einwählen
Schritt 2. Verbindung zum VPN Server
Profile 0
Verbinden
Einfügen
Entfernen
Konfigurieren
Auto-Run when start up:
Profile "
Status: Keine Verbindung
PPTP
ISP VPN

3. Im nächsten Schritt (**Einwahl zum VPN**) geben Sie die Informationen zur Einwahl auf den Server an.

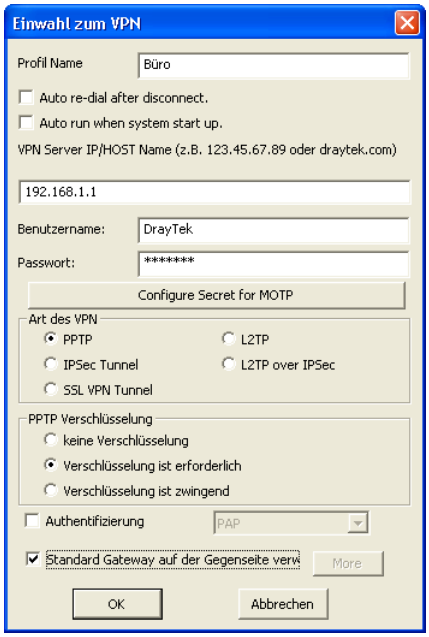
Falls ein IPSec-basierter Dienst wie unten gezeigt gewählt wird ...



... können Sie die Methode für die Zuweisung der IP, die Verschlüsselungsmethode und die Authentifizierungsmethode wählen. Bei Auswahl von Pre-Shared Key sollte dieser mit dem auf dem VPN-Router Konfigurierten übereinstimmen.



Bei Auswahl eines PPP-basierten Dienstes müssen Sie außerdem die IP-Adresse des entfernten VPN-Servers, den Benutzernamen, das Passwort und die Verschlüsselungsmethode angeben. Der Benutzername und das Passwort sollten den auf dem VPN-Router konfigurierten Daten entsprechen. "Use default gateway on remote network" bedeutet, dass alle Pakete des entfernten Hosts zum VPN-Server und von dort ins Internet gesendet werden. So erscheint es, als würde sich der entfernte Host im Unternehmensnetzwerk befinden.

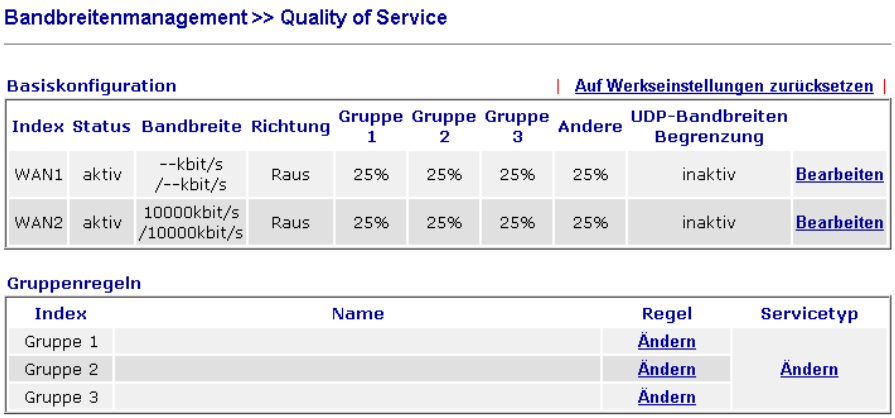


4. Klicken Sie auf **Verbinden**, um die Verbindung aufzubauen. Wenn die Verbindung erfolgreich ist, wird unten rechts eine grüne Lampe angezeigt.

4.3 Beispiel für QoS-Einstellungen

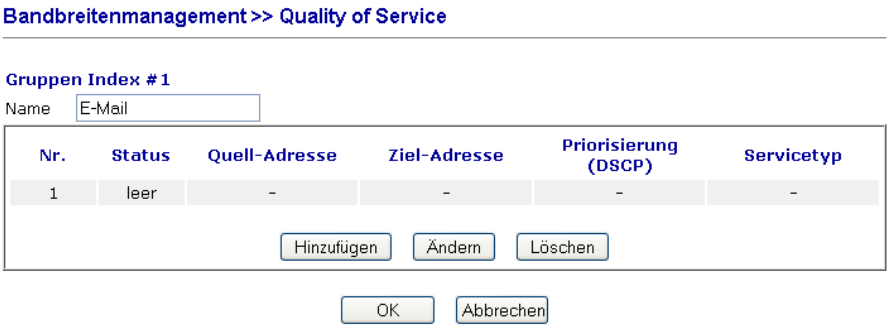
Nehmen wir an, ein Teleworker arbeitet teilweise zu Hause, um seine Kinder beaufsichtigen zu können. Dafür verwendet er seinen Vigor-Router, um sich über HTTPS oder VPN mit dem Server in der Zentrale zu verbinden und so Zugriff auf seine E-Mails und auf die interne Datenbank zu erlangen. Gleichzeitig verwenden die Kinder im Zimmer nebenan Skype.

1. Gehen Sie zu **Bandbreitenmanagement>>Quality of Service.**

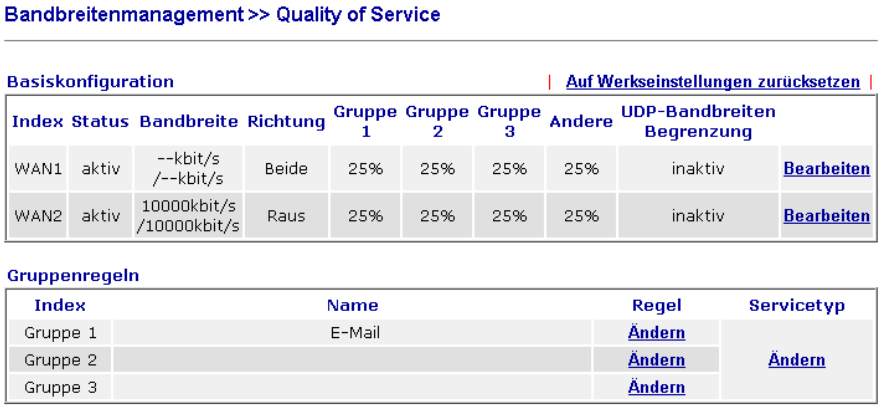

Bandbreitenmanagement >> Quality of Service
Basiskonfiguration
Auf Werkseinstellungen zurücksetzen
Index Status Bandbreite Richtung Gruppe 1 Gruppe 2 Gruppe 3 Andere UDP-Bandbreiten Begrenzung
WAN1 aktiv --kbit/s /--kbit/s Raus 25% 25% 25% 25% inaktiv Bearbeiten
WAN2 aktiv 10000kbit/s /10000kbit/s Raus 25% 25% 25% 25% inaktiv Bearbeiten
Gruppenregeln
Index Name Regel Servicetyp
Gruppe 1 Ändern
Gruppe 2 Ändern Ändern
Gruppe 3 Ändern

2. Klicken Sie bei WAN1 auf **Bearbeiten**. Links muss Aktiv markiert sein. Wählen Sie unter **Richtung Beide**.

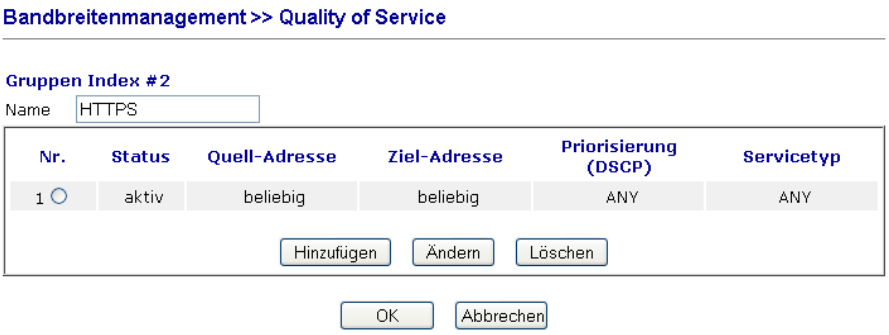
3. Kehren Sie zur vorherigen Seite zurück. Geben Sie den Namen der Indexklasse 1 ein, indem Sie auf **Bearbeiten** klicken. Geben Sie für Klasse 1 den Namen "**E-Mail**" ein.


Bandbreitenmanagement >> Quality of Service
Gruppen Index #1
Name E-Mail
Nr. Status Quell-Adresse Ziel-Adresse Priorisierung (DSCP) Servicetyp
1 leer - - - -
Hinzufügen Ändern Löschen
OK Abbrechen

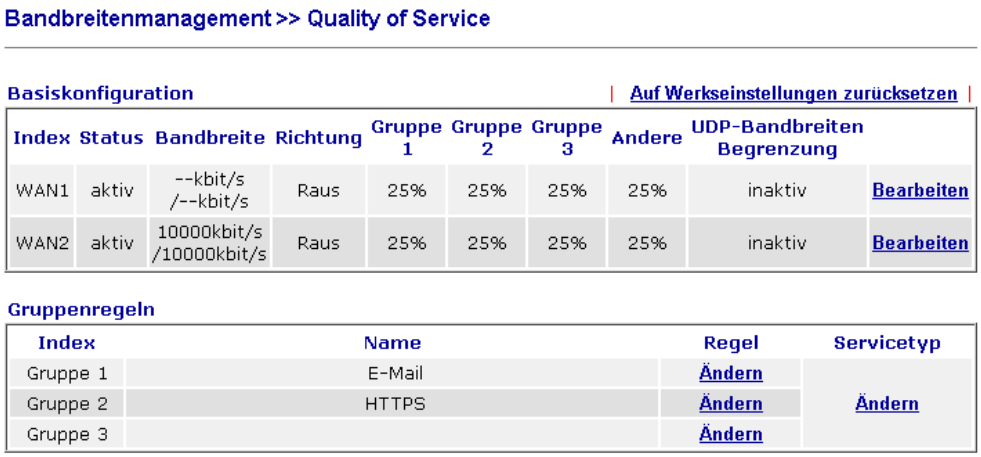
4. In diesem Index kann der Benutzer die reservierte Bandbreite (z.B. 25%) für **E-Mail** über die Protokolle POP3 und SMTP bestimmen.


Bandbreitenmanagement >> Quality of Service
Basiskonfiguration | Auf Werkseinstellungen zurücksetzen |
Index Status Bandbreite Richtung Gruppe 1 Gruppe 2 Gruppe 3 Andere UDP-Bandbreiten Begrenzung
WAN1 aktiv --kbit/s /--kbit/s Beide 25% 25% 25% 25% inaktiv Bearbeiten
WAN2 aktiv 10000kbit/s /10000kbit/s Raus 25% 25% 25% 25% inaktiv Bearbeiten
Gruppenregeln
Index Name Regel Servicetyp
Gruppe 1 E-Mail Ändern
Gruppe 2 Ändern Ändern
Gruppe 3 Ändern

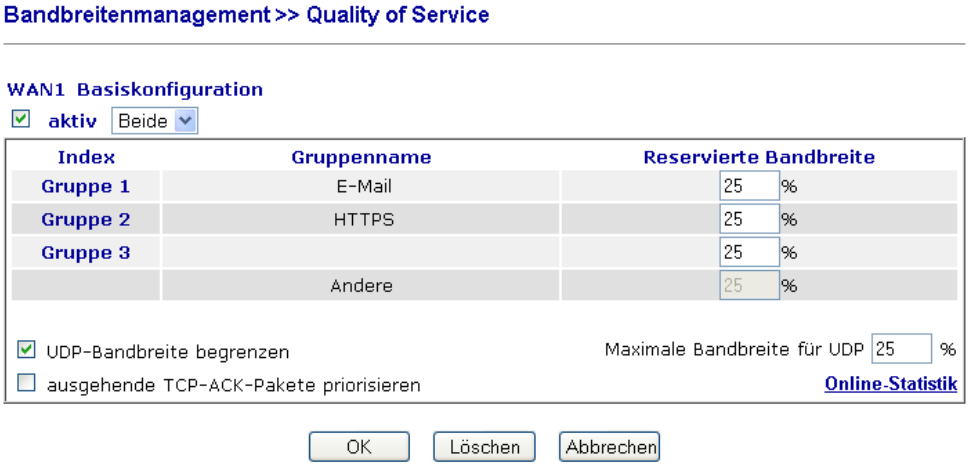
5. Kehren Sie zur vorherigen Seite zurück. Geben Sie den Namen der Indexklasse 2 ein, indem Sie auf **Bearbeiten** klicken. In diesem Index kann der Benutzer die reservierte Bandbreite für **HTTPS** bestimmen. Klicken Sie auf **OK**.


Bandbreitenmanagement >> Quality of Service
Gruppen Index #2
Name HTTPS
Nr. Status Quell-Adresse Ziel-Adresse Priorisierung (DSCP) Servicetyp
1 aktiv beliebig beliebig ANY ANY
Hinzufügen Ändern Löschen
OK Abbrechen

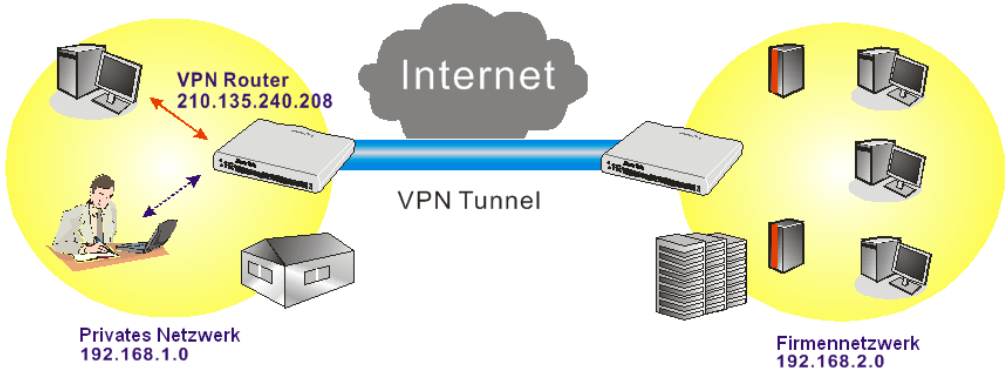
6. Klicken Sie bei WAN1 auf **Bearbeiten**.

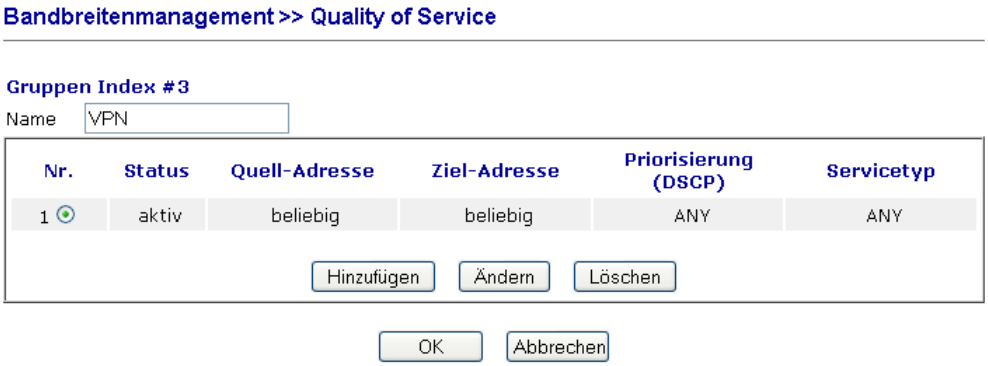

Bandbreitenmanagement >> Quality of Service
Basiskonfiguration
Auf Werkseinstellungen zurücksetzen
Index Status Bandbreite Richtung Gruppe 1 Gruppe 2 Gruppe 3 Andere UDP-Bandbreiten Begrenzung
WAN1 aktiv --kbit/s /--kbit/s Raus 25% 25% 25% 25% inaktiv Bearbeiten
WAN2 aktiv 10000kbit/s /10000kbit/s Raus 25% 25% 25% 25% inaktiv Bearbeiten
Gruppenregeln
Index Name Regel Servicetyp
Gruppe 1 E-Mail Ändern
Gruppe 2 HTTPS Ändern Ändern
Gruppe 3 Ändern

7. Klicken Sie unten auf **UDP-Bandbreite begrenzen**, um zu vermeiden, dass übermäßiger UDP-Verkehr VoIP oder andere Anwendungen beeinträchtigt. Klicken Sie auf **OK**.



8. Falls sich der Teleworker über einen Host-zu-Host-Tunnel mit der Zentrale verbunden hat (siehe detaillierte Anweisungen in Kapitel 3 "VPN"), kann er hierfür einen Index einrichten. Geben Sie die Bezeichnung der Klasse von Index 3 an. In diesem Index kann die reservierte Bandbreite für einen VPN-Tunnel bestimmt werden.

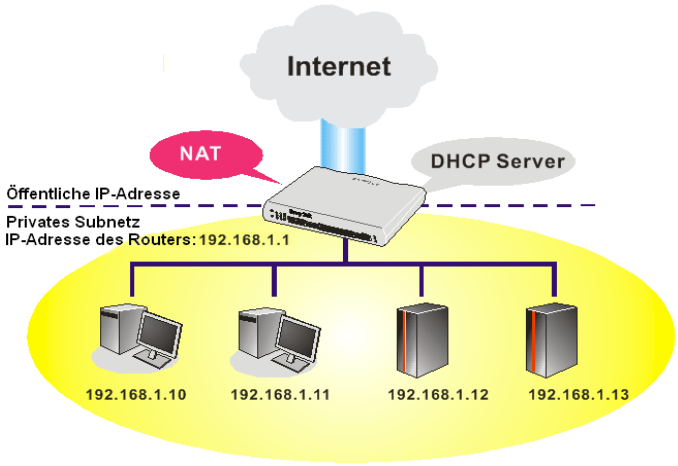




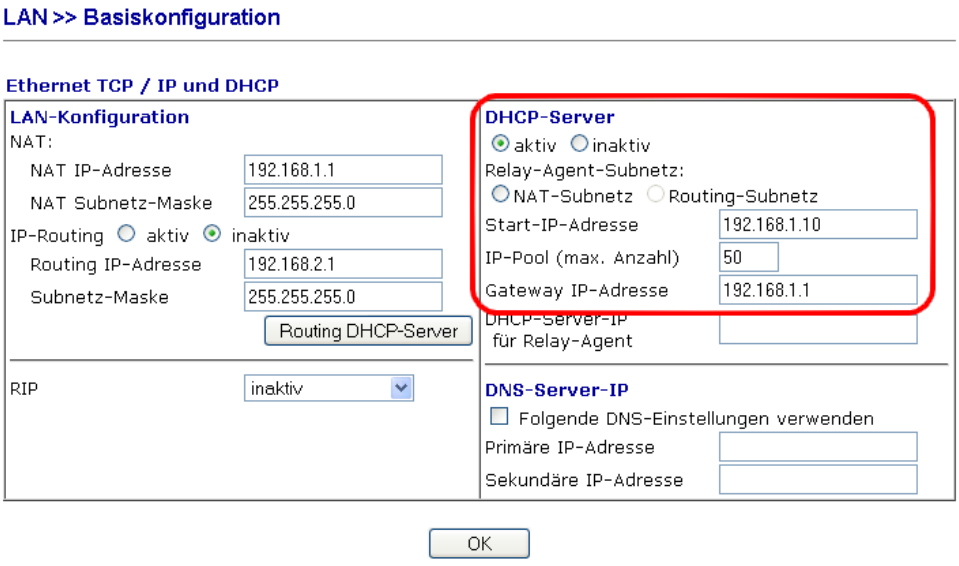
9. Klicken Sie auf **Bearbeiten**, um das folgende Fenster zu öffnen. Markieren Sie zunächst**Aktiv** und klicken Sie dann auf **Bearbeiten** neben **Quell-Adresse**, um die Subnetzadresse des Teleworkers einzustellen. Klicken Sie auf **Bearbeiten** neben **Ziel-Adresse**, um die IP-Adresse der Zentrale einzugeben. Lassen Sie alle anderen Felder, wie sie sind, und klicken Sie auf **OK**.

4.4 LAN – Einrichtung mit NAT

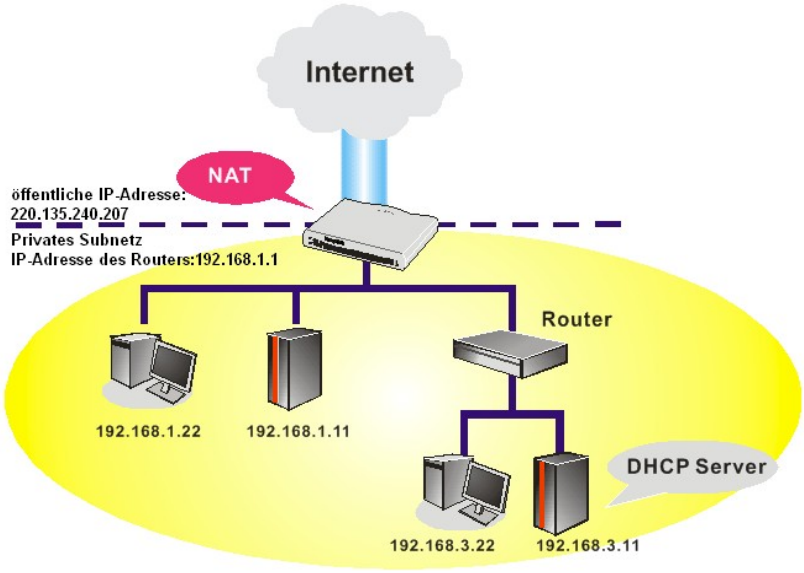
Die folgende Abbildung zeigt die Standardeinstellungen und ein Einsatzbeispiel. Die Standardwerte für private IP-Adresse/Subnetz-Maske sind 192.168.1.1/255.255.255.0. Der eingebaute DHCP-Server ist so konfiguriert, dass er jedem NAT-Host eine IP-Adresse zwischen 192.168.1.x und 192.168.1.10 zuweist.



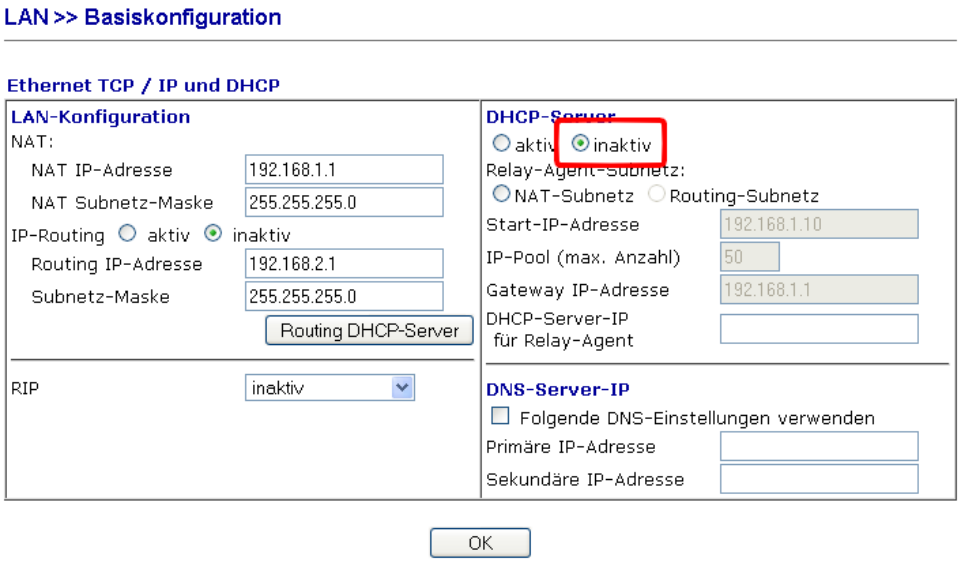
Sie können die rot eingerahmten Einstellungen den Anforderungen Ihrer NAT-Nutzung anpassen.



Um im Netzwerk einen anderen DHCP-Server als den eingebauten DHCP-Server des Vigor-Routers zu verwenden, müssen Sie die Einstellungen wie unten gezeigt ändern.



Sie können die rot eingerahmten Einstellungen den Anforderungen Ihrer NAT-Nutzung anpassen.

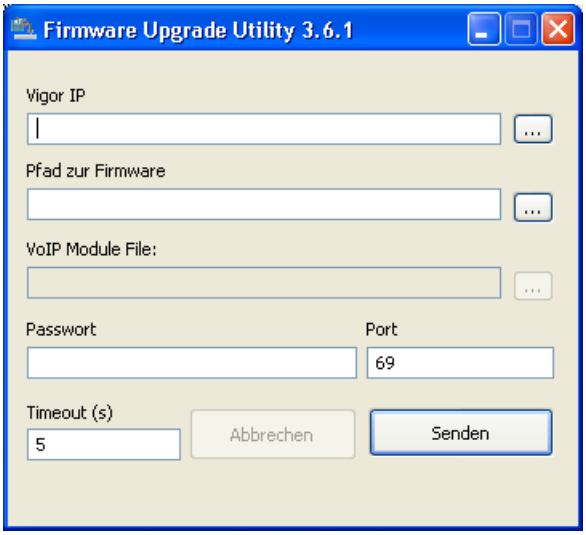


4.5 Firmware des Routers aktualisieren

Um Ihre Router-Firmware zu aktualisieren müssen Sie die Router Tools installieren. Speichern Sie die Datei **RTSxxx.exe** auf Ihrem Rechner. Merken Sie sich den Speicherort der ausführbaren Datei.

1. Gehen Sie zu **www.draytek.de**.
2. Gehen Sie zu **Downloads**. Klicken Sie auf **Firmware**. Suchen Sie nach Ihrem Modell und laden Sie die aktualisierte Firmware für Ihren Router herunter.
3. Gehen Sie zu **Downloads**. Klicken Sie auf **Tools / Utilities**.
4. Laden Sie das Firmware Upgrade Utility herunter.

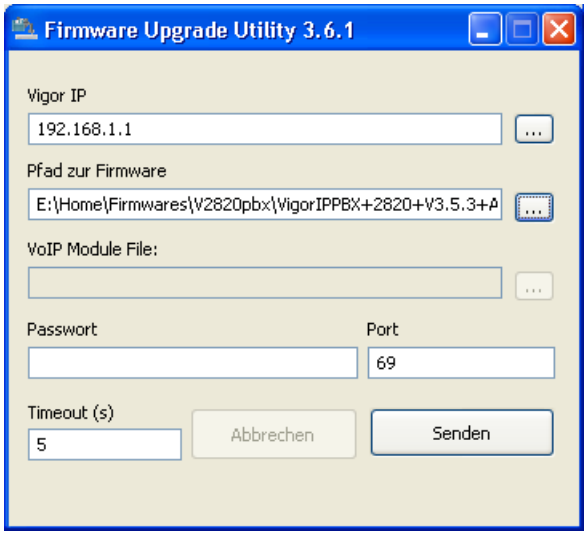
5. Entpacken Sie die heruntergeladene Datei und führen Sie Firmwareupgrade.exe aus.



6. Geben Sie Ihre Router-IP ein, normalerweise **192.168.1.1**.

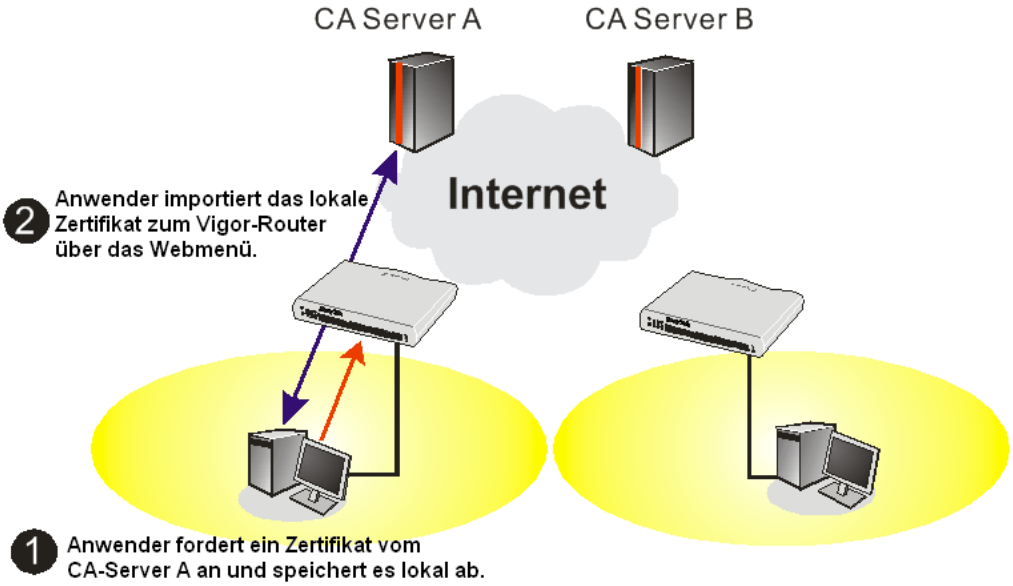
7. Klicken Sie auf die Taste rechts neben dem Feld, das die Firmware-Datei enthält. Wählen Sie die Datei, die Sie von der Web-Site des Herstellers heruntergeladen haben. Sie werden zwei Dateien mit unterschiedlichen Erweiterungen sehen, **xxxx.all** (erhält die benutzerspezifischen Einstellungen) **u**nd **xxxx.rst** (setzt alle benutzerspezifischen Einstellungen auf die Werkseinstellungen zurück). Wählen Sie die benötigte Datei.

8. Klicken Sie auf **Senden**.



9. Die erfolgreiche Aktualisierung wird mit einer Nachricht bestätigt.

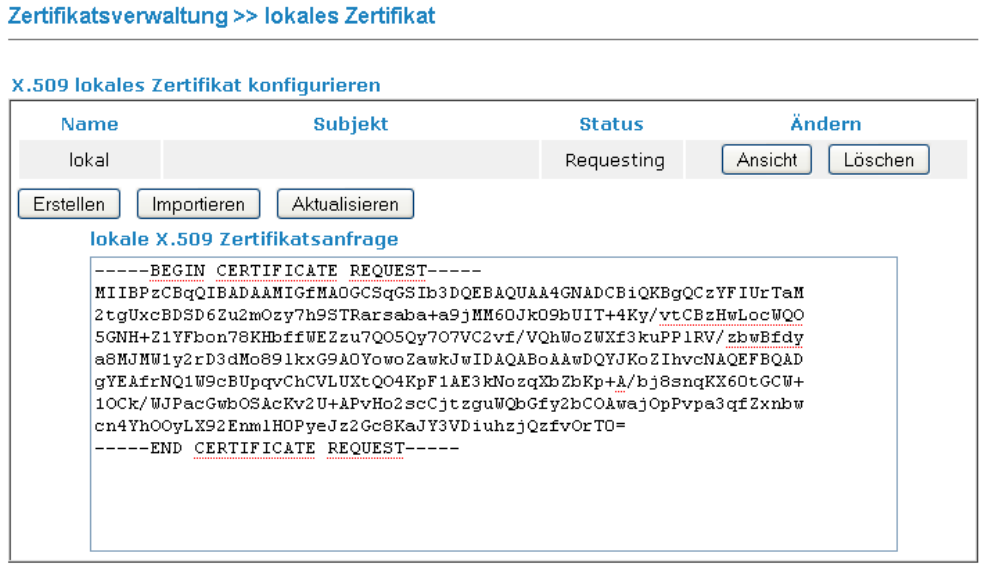
4.6 Zertifikat von einem CA-Server oder Windows CA-Server anfordern


CA Server A
CA Server B
Internet
2
Anwender importiert das lokale Zertifikat zum Vigor-Router über das Webmenü.
1
Anwender fordert ein Zertifikat vom CA-Server A an und speichert es lokal ab.

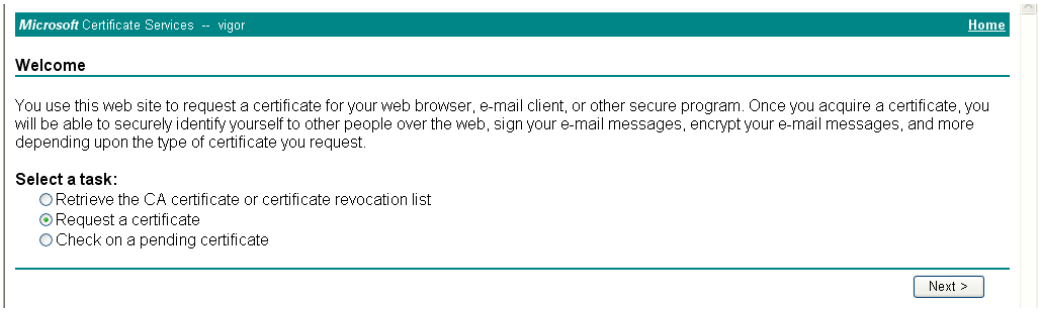
1. Gehen Sie zur **Zertifikatsverwaltung** und wählen Sie **Lokales Zertifikat**.

2. Klicken Sie auf **Erstellen**, um ein Zertifikat zu erstellen. Geben Sie die Daten ein, die zur Erstellung eines Zertifikats erforderlich sind.

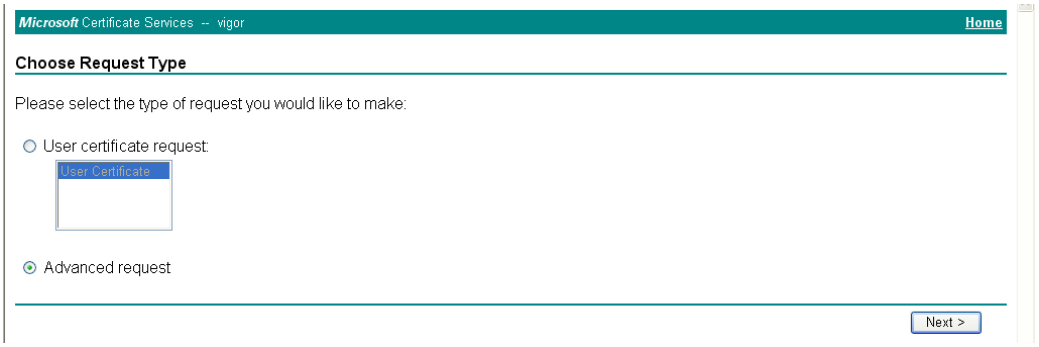
3. Kopieren und speichern Sie die lokale X.509 Zertifikatsanfrage als Textdatei und bewahren Sie sie für späteren Gebrauch auf.



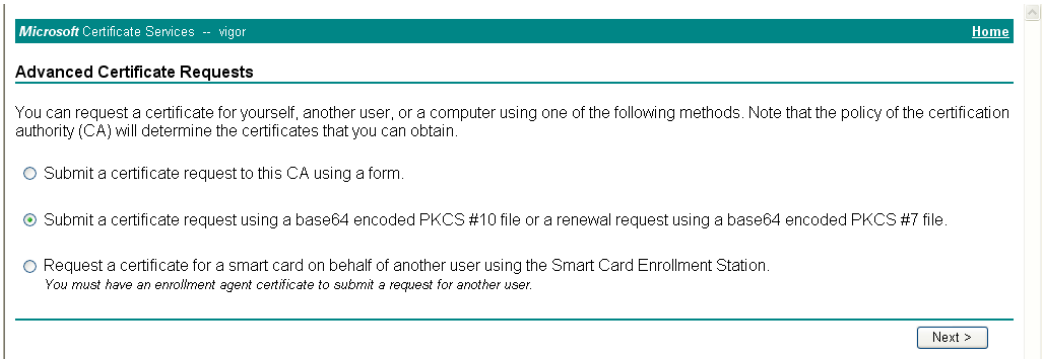
4. Verbinden Sie sich über den Web-Browser mit dem CA-Server. Folgen Sie den Anweisungen, um die Anfrage zu stellen. Das folgende Beispiel zeigt einen Windows 2000 CA-Server. Wählen Sie **Ein Zertifikat anfordern** und klicken Sie auf **Weiter**.


Microsoft Certificate Services -- vigor
Home
Welcome
You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the type of certificate you request.
Select a task:
Retrieve the CA certificate or certificate revocation list
Request a certificate
Check on a pending certificate
Next >

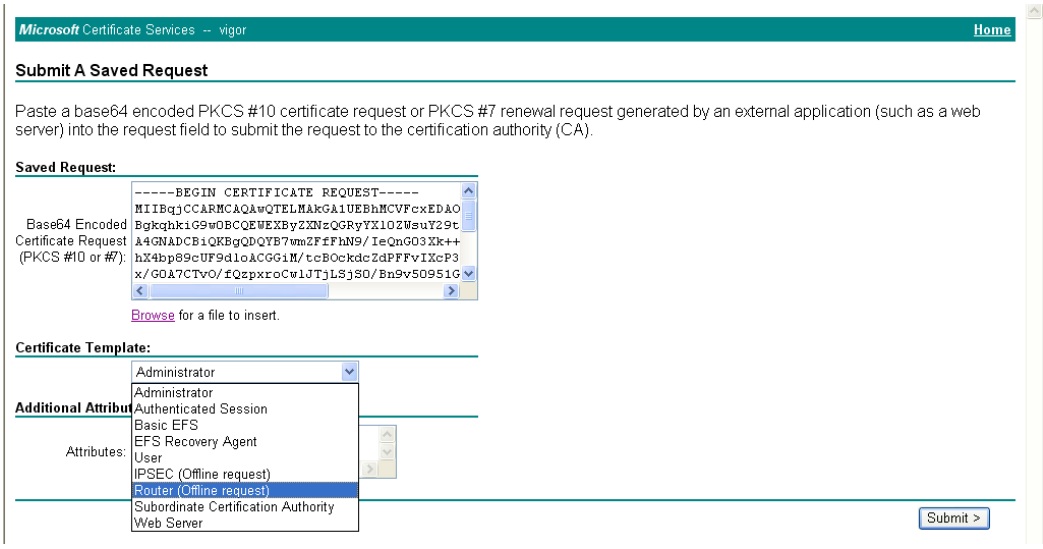
Klicken Sie unter **Anforderungstyp wählen** auf **Erweiterte Anforderung**.



Wählen Sie **Senden Sie eine Zertifikatsanforderung ein, die eine Base64-codierte PKCS10-Datei verwendet, oder eine Erneuerungsanforderung, die eine Base64-codierte PKCS7-Datei verwendet**.

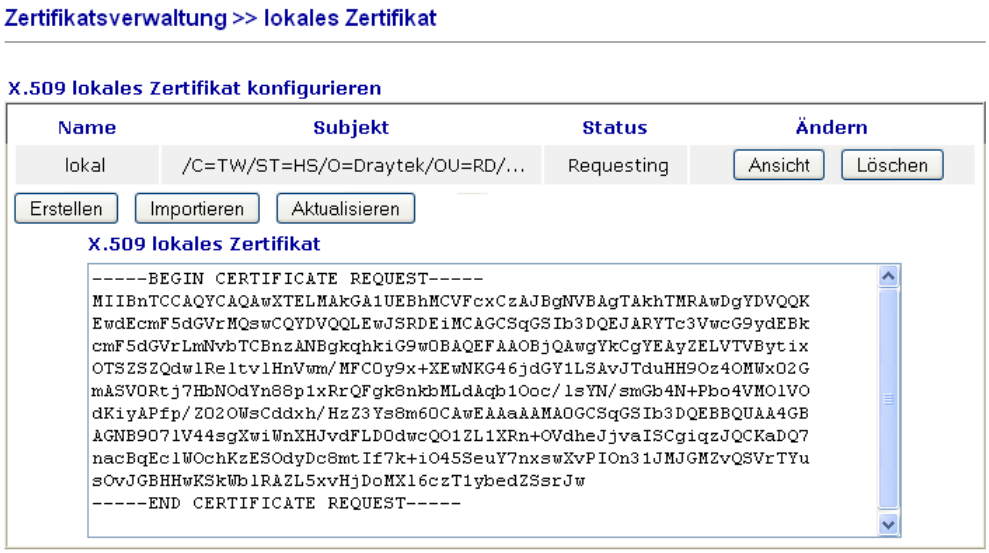


Importieren Sie die lokale X.509 Zertifikatsanforderungsdatei. Wählen Sie unten **Router (Offline request)** oder **IPSec (Offline request)**.



Nach Absenden der Anforderung stellt der Server ein Zertifikat aus. Wählen Sie **Base64-codiertes Zertifikat** und **Download des Zertifizierungsstellenzertifikats**. Speichern Sie das Zertifikat (.cer-Datei) ab.

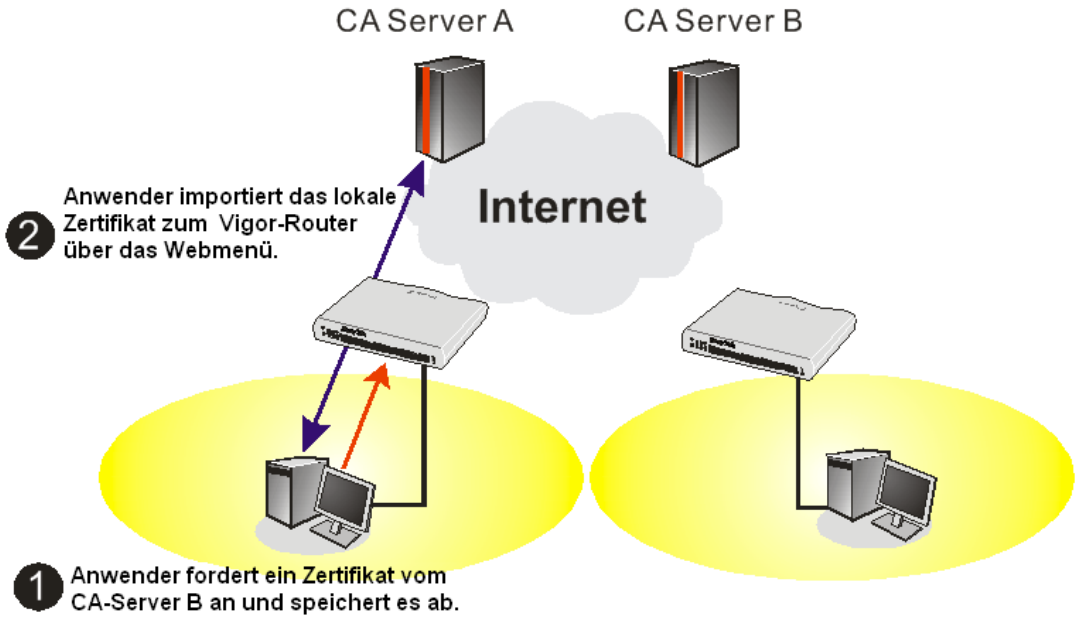
5. Auf dem Vigor-Router gehen Sie zu **Lokales Zertifikat**. Klicken Sie auf **Importieren** und wählen Sie die entsprechende Datei, um das Zertifikat (.cer-Datei) auf dem Vigor-Router zu importieren. Klicken Sie nach Abschluss auf Aktualisieren; im Feld unten erscheint "BEGIN CERTIFICATE ...".



6. Sie können die Details des Zertifikats kontrollieren, indem Sie auf **Ansicht** klicken.

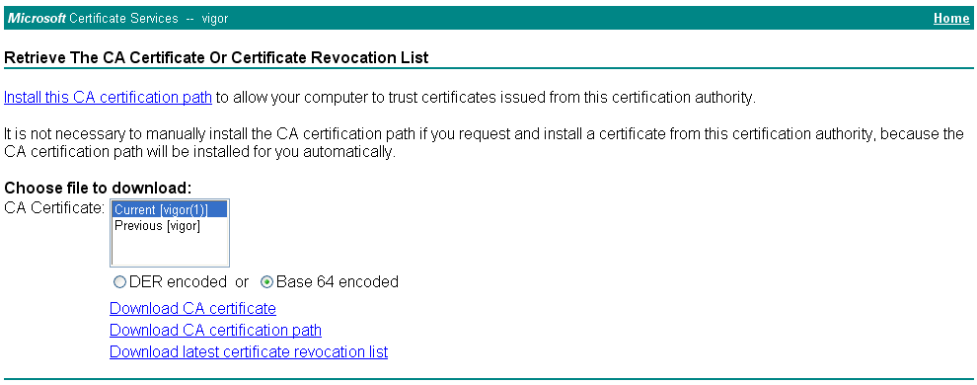
Name : Local
Issuer : /C=US/CN=vigor
Subject : /emailAddress=press@draytek.com/C=TW/O=Draytek
Subject Alternative Name : DNS:draytek.com
Valid From : Aug 30 23:08:43 2005 GMT
Valid To : Aug 30 23:17:47 2007 GMT

4.7 CA-Zertifikat von Windows CA-Server anfordern und als vertrauenswürdiges Zertifikat setzen

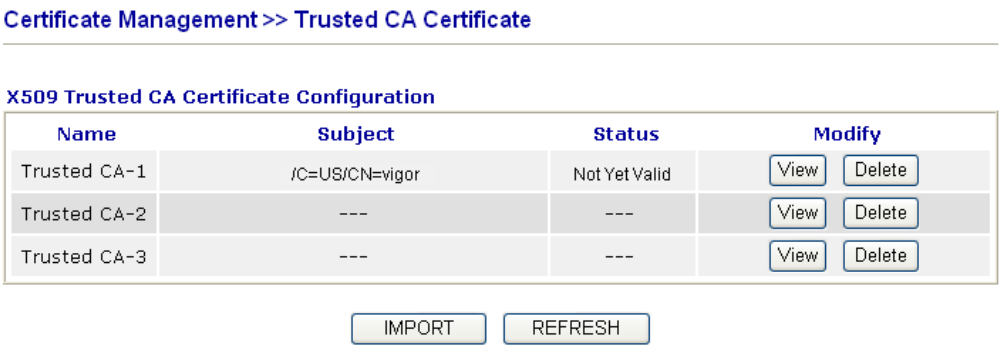

CA Server A
CA Server B
Internet
2
Anwender importiert das lokale Zertifikat zum Vigor-Router über das Webmenü.
1
Anwender fordert ein Zertifikat vom CA-Server B an und speichert es ab.

1. Benutzen Sie den Web-Browser, um sich mit dem CA-Server zu verbinden, von dem Sie ein CA-Zertifikat herunterladen möchten. Klicken Sie auf **Download eines Zertifizierungstellenzertifikats, einer Zertifikatkette oder einer Sperrliste**.

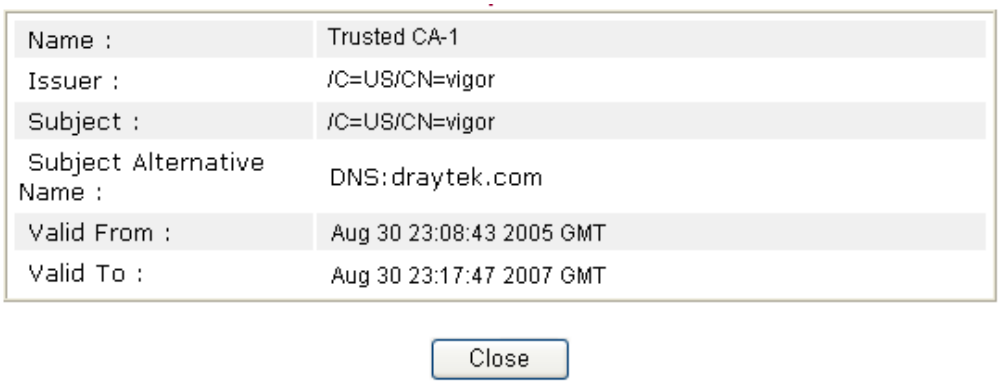
2. Unter **Datei zum Downloaden auswählen** klicken Sie auf das CA-Zertifikat **Current** und auf **Base64-codiert** und dann auf **Download des Zertifizierungsstellenzertifikats**, um die .cer-Datei zu speichern.


Microsoft Certificate Services -- vigor
Home
Retrieve The CA Certificate Or Certificate Revocation List
Install this CA certification path to allow your computer to trust certificates issued from this certification authority.
It is not necessary to manually install the CA certification path if you request and install a certificate from this certification authority, because the CA certification path will be installed for you automatically.
Choose file to download:
CA Certificate:
Current [vigor(1)]
Previous [vigor]
DER encoded or Base 64 encoded
Download CA certificate
Download CA certification path
Download latest certificate revocation list

3. Auf dem Vigor-Router gehen Sie zu **Vertrauenswürdiges CA-Zertifikat**. Klicken Sie auf **Importieren** und wählen Sie die entsprechende Datei, um das Zertifikat (.cer-Datei) auf dem Vigor-Router zu importieren. Klicken Sie nach Abschluss auf Aktualisieren, damit die Information wie folgt angezeigt wird.



4. Sie können die Details des Zertifikats kontrollieren, indem Sie auf **Ansicht** klicken.



Hinweis: Bevor Sie das Zertifikat konfigurieren, stellen Sie bitte unter **Systemmanagement >> Zeit und Datum** die aktuelle Zeit des Routers ein.

Kapitel 5: Referenz - erweiterte Web-Konfiguration

Nach der grundlegenden Konfiguration des Routers haben Sie Zugriff auf das Internet. Dieses Kapitel enthält detaillierte Informationen zur erweiterten Konfiguration dieses Routers für Benutzer, deren Bedürfnisse weitere Anpassungen erfordern. Weitere Anwendungsfälle werden in Kapitel 4 beschrieben.

5.1 WAN

Der **Schnellstart-Assistent** bietet Benutzern eine einfache Möglichkeit, den Verbindungsmodus für den Router schnell einzurichten. Falls Sie weitere Einstellungen für verschiedene WAN-Modi konfigurieren möchten, gehen Sie bitte ins Menü **WAN** und klicken auf **Einwahl ins Internet**.

5.1.1 Grundlagen des Internet Protocol (IP) Netzwerks

IP ist die Abkürzung für Internet Protocol. Jedes Gerät in einem IP-basierten Netzwerk (z.B. Router, Printserver und Host-PCs) benötigt eine IP-Adresse, welche dessen Standort im Netzwerk bestimmt. Um Adressenkonflikte zu vermeiden, sind IP-Adressen öffentlich beim Network Information Center (NIC) registriert. Eine unverwechselbare IP-Adresse ist für Geräte im öffentlichen Netzwerk unbedingt erforderlich, nicht jedoch in den privaten lokalen TCP/IP-Netzwerken (LANs), da auf diese kein öffentlicher Zugriff nötig ist. Dies können beispielsweise Host-PCs sein, die von einem Router verwaltet werden. Aus diesem Grunde hat das NIC gewisse Adressen reserviert, die niemals öffentlich registriert werden. Diese werden als ***private*** IP-Adressen bezeichnet und umfassen die folgenden Bereiche:

Von 10.0.0.0 bis 10.255.255.255
Von 172.16.0.0 bis 172.31.255.255
Von 192.168.0.0 bis 192.168.255.255

Öffentliche IP-Adressen und private IP-Adressen

Der Router, der für die Verwaltung und den Schutz seines LANs verantwortlich ist, verbindet Gruppen von Host-PCs. Der eingebaute DHCP-Server des Vigor-Routers weist jedem dieser PCs eine private IP-Adresse zu. Der Router selbst verwendet für die Kommunikation mit den lokalen Hosts standardmäßig die **private IP**-Adresse 192.168.1.1. Zur Kommunikation mit anderen Netzwerkgeräten verwendet der Vigor-Router eine **öffentliche IP**-Adresse. Beim Durchfluss der Daten wandelt die Network Address Translation (NAT) Funktion des Routers öffentliche/private Adressen um, und die Pakete werden dem entsprechenden Host-PC im LAN ausgeliefert. Auf diese Weise können alle Host-PCs einen gemeinsamen Internetanschluss nutzen.

Öffentliche IP-Adresse vom ISP beziehen

Beim Einsatz für ADSL muss für eine erfolgreiche Verbindung von Endgeräten PPP-Authentifizierung und Autorisierung verwendet werden. Point-to-Point Protocol over Ethernet (PPPoE) verbindet ein Netzwerk von Hosts über ein Zugriffsgerät mit einem Fernzugriffskonzentrator. Dieser Ansatz vereinfacht die Nutzung für Benutzer. Je nach Benutzeranforderung ermöglicht dies die Zugriffskontrolle, Abrechnung und Angabe der Dienstart (ToS).

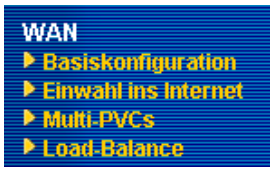
Wenn sich ein Router mit Ihrem ISP verbindet, finden verschiedene Verbindungsprozesse statt, um eine Verbindung anzufordern. Dann wird eine Sitzung aufgebaut. Ihr Benutzername und Ihr Passwort werden über **PAP** oder **CHAP** mit dem **RADIUS**-Authentifizierungssystem authentifiziert. Normalerweise werden die IP-Adresse, die DNS-Server und andere Informationen vom ISP zugewiesen.

5.1.2 Netzwerkverbindung über 3G USB-Modem

Im Hinblick auf die zunehmende Beliebtheit der mobilen 3G-Kommunikation über Access Points bietet der Vigor2820 die Funktionalität einer 3G-Netzwerkverbindung. So kann ein 3G-USB-Modem an den USB-Port des Vigor2820 angeschlossen werden, wobei HSDPA/UMTS/EDGE/GPRS/GSM sowie zukünftige 3G-Standards (HSUPA usw.) unterstützt werden. Vigor2820 mit 3G-USB-Modem ermöglicht Ihnen, von jedem beliebigen Ort (z.B. Auto, Außenbereich) 3G-Signale zu empfangen und die vorhandene Bandbreite mit anderen Benutzern zu teilen. Benutzer können für den Zugriff auf das Internet die vier LAN-Ports des Routers nutzen. Außerdem können sie über die 802.11n Wireless-Funktion des Vigor2820n auf das Internet zugreifen und Funktionalitäten der Vigor2820-Serie wie Firewall, Bandbreitenmanagement, VPN und VoIP nutzen.

Nach Anschluss am Router wird das 3G USB-Modem als zweiter WAN-Port betrachtet. Die WAN1-Schnittstelle (Ethernet) kann weiterhin verwendet werden, und der Router kann für Load-Balance konfiguriert werden. Das 3G USB-Modem an WAN2 kann auch als Backup verwendet werden. In diesem Falle benutzt der Router automatisch 3.5G, falls WAN1 nicht verfügbar ist. Die unterstützten 3G USB-Modems sind auf der Draytek-Website aufgelistet. Weitere Informationen sind unter www.draytek.de erhältlich.

Die folgende Abbildung zeigt die Menüeinträge für die Einwahl ins Internet:



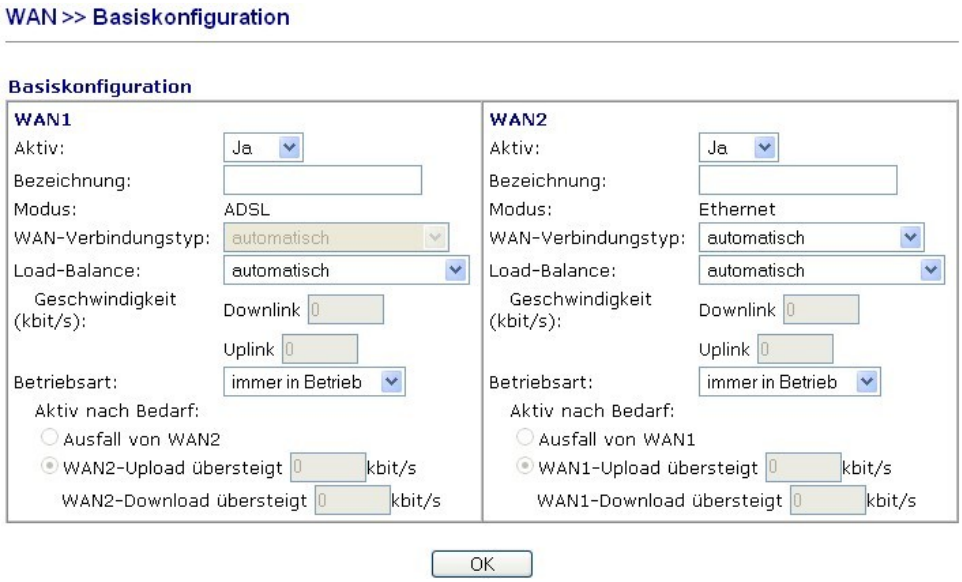
5.1.3 Basiskonfiguration

In diesem Teil werden einige allgemeine Interneteinstellungen sowie die Verbindungsmodi für WAN1 und WAN2 detailliert vorgestellt.

Dieser Router unterstützt zwei WANs. Durch Kombination der Bandbreiten beider WANs kann die Übertragung im Netzwerk beschleunigt werden. Die WAN-Ports können sich mit verschiedenen ISPs verbinden, selbst wenn diese Ihre Telekommunikationsleistungen über unterschiedliche Technologien bereitstellen (z.B. DSL, Kabelmodem usw.). Sollte die Verbindung über einen der ISPs gestört sein, wird der gesamte Verkehr über den anderen, funktionierenden Port geleitet, um den ordnungsgemäßen Betrieb sicherzustellen. Bitte stellen Sie WAN1 und WAN2 entsprechend ein.

Dieser Dialog dient der allgemeinen Einrichtung von WAN1 und WAN2

Hinweis: Standardmäßig ist sowohl WAN1 als auch WAN2 aktiviert.

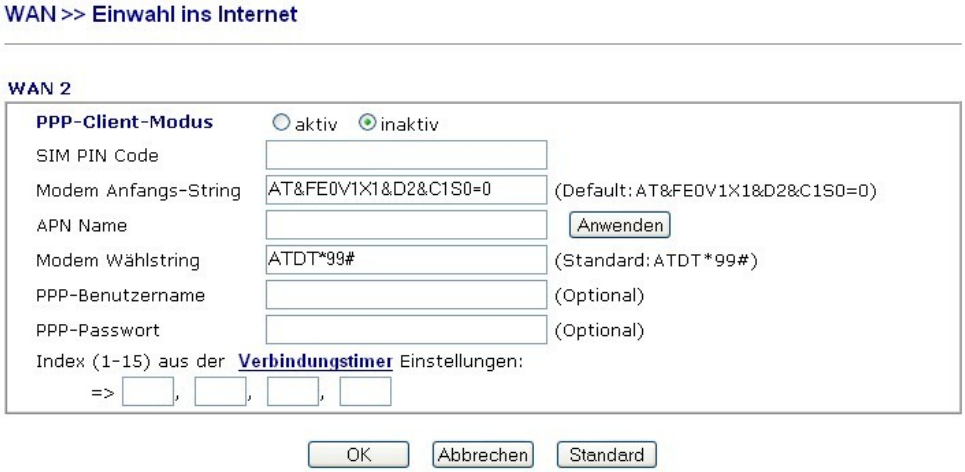


Aktiv - Wählen Sie **Ja**, um zu den Einstellungen für diese WAN-Schnittstelle zu gelangen. Wählen Sie **Nein**, um die Einstellungen für diese WAN-Schnittstelle zu deaktivieren.

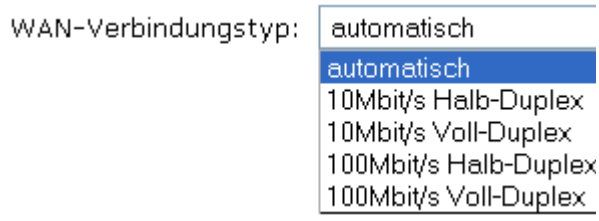
Angezeigter Name - Geben Sie die Beschreibung der WAN1-/WAN2-Schnittstelle ein.

Modus - Bei WAN1 findet die physikalische Verbindung über den ADSL-Port statt; die physikalische Verbindung bei WAN2 hingegen findet über einen Ethernet- (P1) oder USB-Port statt. Dies kann nicht geändert werden.

Um eine 3G-Netzwerkverbindung über ein 3G USB-Modem zu ermöglichen, wählen **3G USB-Modem** als Modus in **WAN2**. Dann gehen Sie zu **WAN>> Einwahl ins Internet**. Das 3G USB-Modem ist für WAN2 verfügbar. Sie können **PPP** als Verbindungsart wählen und mit der Konfiguration fortfahren.



WAN-Verbindungstyp - Diese Einstellung ist nur für WAN2 verfügbar. Sie können den Verbindungstyp für WAN2 angeben oder **Automatisch -** wählen, damit er vom System automatisch festgestellt wird.



Load-Balance - Falls Sie die tatsächliche Bandbreite Ihrer WAN-Schnittstelle kennen, wählen Sie bitte die Einstellung **Abhängig vom Anschluss**. Andernfalls wählen Sie bitte **Automatisch**, um den Router die geeignete

Load-Balance bestimmen zu lassen.

Geschwindigkeit - Falls Sie **Abhängig vom Anschluss** als **Load-Balance** wählen, geben Sie bitte die Download- und Upload-Geschwindigkeiten für WAN1/WAN2 an. Die Einheit ist kbit/s.

Betriebsart - Wählen Sie **Immer in Betrieb**, um die WAN-Verbindung (WAN1/WAN2) dauerhaft aufrecht zu erhalten, oder **Aktiv nach Bedarf**, um die WAN-Verbindung (WAN1/WAN2) bei Bedarf zu aktivieren.

Falls Sie Aktiv nach Bedarf wählen, können Sie die max. Leerlaufzeit für die Zugriffsarten PPPoE und PPTP in den Einstellungen unter WAN>>Einwahl ins Internet konfigurieren. Außerdem können Sie drei weitere Optionen für verschiedene Zwecke konfigurieren.

Ausfall von WAN2 – Die WAN1-Verbindung wird aktiviert, falls WAN2 ausfällt.

WAN2-Upload übersteigt XX kbit/s – Die WAN1-Verbindung wird aktiviert, sobald die WAN2-Upload-Geschwindigkeit den hier eingestellten Wert über einen Zeitraum von mehr als 15 Sekunden übersteigt.

WAN2-Download übersteigt XX kbit/s – Die WAN1-Verbindung wird aktiviert, sobald die WAN2-Download-Geschwindigkeit den hier eingestellten Wert über einen Zeitraum von mehr als 15 Sekunden übersteigt.

Ausfall von WAN1 – Die WAN2-Verbindung wird aktiviert, falls WAN1 ausfällt.

WAN1-Upload übersteigt XX kbit/s – Die WAN2-Verbindung wird aktiviert, sobald die WAN1-Upload-Geschwindigkeit den hier eingestellten Wert über einen Zeitraum von mehr als 15 Sekunden übersteigt.

WAN1-Download übersteigt XX kbit/s – Die WAN2-Verbindung wird aktiviert, sobald die WAN1-Download-Geschwindigkeit den hier eingestellten Wert über einen Zeitraum von mehr als 15 Sekunden übersteigt.

5.1.4 Einwahl ins Internet

Da der Router die Einrichtung von zwei WAN-Verbindungen erlaubt, kann der Benutzer für die Einwahl ins Internet verschiedene WAN-Einstellungen (für WAN1/WAN2) konfigurieren. Aufgrund der unterschiedlichen Modi von WAN1 und WAN2 unterscheiden sich die Verbindungsarten für diese zwei Verbindungen leicht voneinander.

WAN >> Einwahl ins Internet

Einwahl ins Internet

Index	Bezeichnung	Modus	Übersicht
WAN1		ADSL	Kanal: 1, VPI: 1, VCI: 32, Protokoll: PPPoE/LLC/SNAP, Modulation: Multimode, dynamische IP
WAN2		Ethernet	DHCP-Client

Index - Zeigt die WAN-Modi an, die dieser Router unterstützt. WAN1 ist die Standard-WAN-Schnittstelle für die Einwahl ins Internet. WAN2 ist die optionale WAN-Schnittstelle für die Einwahl in das Internet, wenn WAN1 aus irgendeinem Grund nicht verfügbar sein sollte.

Angezeigter Name - Zeigt den in der Basiskonfiguration eingegebenen WAN1-/WAN2-Namen an.

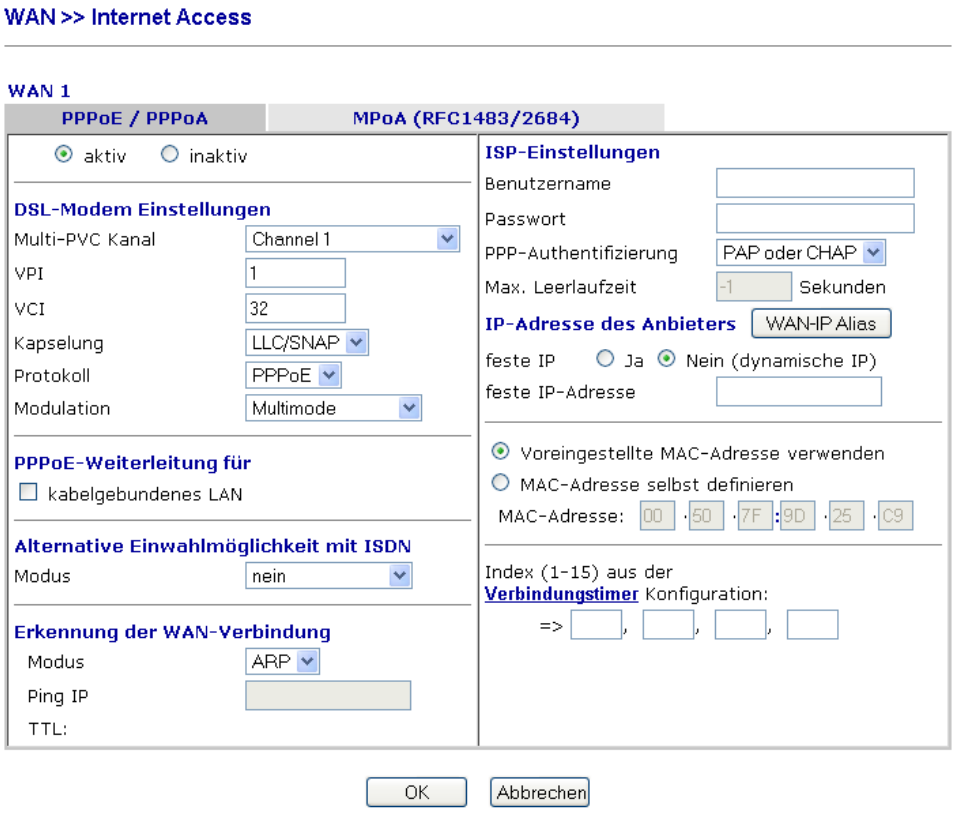
Modus - Zeigt den physikalischen Port für WAN1/WAN2 an.

Übersicht - Zeigt eine Übersicht der Konfiguration der WAN1-/WAN2-Schnittstelle.

WAN1 und WAN2 unterstützen verschiedene Protokolle. WAN1 unterstützt PPPoE/PPPoA und MPoA. WAN2 unterstützt PPPoE, feste oder dynamische IP und PPTP. Je nach Verbindungsart wählen Sie bitte die entsprechende WAN-Schnittstellenverbindung, um die Einzelheiten zu konfigurieren.

PPPoE/PPPoA für WAN1

Um **PPPoE/PPPoA** als das Zugriffsprotokoll des Internets zu verwenden, wählen Sie den **PPPoE/PPPoA**-Modus. Der folgende Dialog erscheint:



Aktiv/Inaktiv - Klicken Sie auf **Aktiv**, um diese Funktion zu aktivieren. Klicken Sie auf **Inaktiv**, so wird diese Funktion geschlossen, und alle auf dieser Seite vorgenommenen Einstellungen werden verworfen.

DSL-Modemeinstellungen - Konfigurieren Sie die für Ihren ISP erforderlichen DSL-Parameter. Diese sind unerlässlich, um zu Ihrem ISP eine DSL-Verbindung aufzubauen.

Multi-PVC-Kanal - Die hier angezeigte Auswahl wird von der Seite **Einwahl ins Internet** – **Multi PVC** bestimmt. **M-PVC-Kanal auswählen** bedeutet, dass keine Auswahl markiert wird.

VPI - Geben Sie den vom ISP mitgeteilten Wert ein.

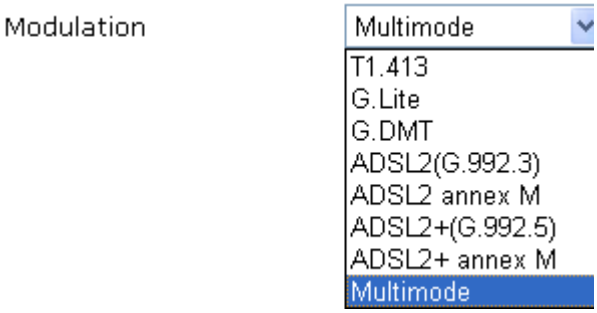
VCI - Geben Sie den vom ISP mitgeteilten Wert ein.

Kapselung - Dropdown-Liste zur Auswahl des vom ISP bestimmten Typs.

Protokoll - Dropdown-Liste zur Auswahl des vom ISP bestimmten Protokolls.

Falls Sie das Protokoll bereits mit dem **Schnellstart-Assistent**en eingestellt haben, brauchen Sie hier keine Einstellungen zu ändern.

Modulation – Die Standardeinstellung ist **Multimode**. Wählen Sie die Einstellung, die Ihren Bedürfnissen entspricht.



PPPoE Pass-Through - Der Router bietet die Möglichkeit, eine PPPoE-Wählverbindung einzurichten. Außerdem können Sie die PPPoE-Verbindung über den Vigor-Router direkt von den lokalen Clients zum ISP aufbauen. Falls das PPPoA-Protokoll ausgewählt ist, wird das vom PC übertragene PPPoE-Paket in ein PPPoA-Paket umgewandelt und an den WAN-Server übermittelt. Über diese Weiterleitung kann der PC auf das Internet zugreifen.

Kabelgebundenes LAN – Falls Sie dieses Kästchen markieren, können PCs im gleichen Netzwerk für den Internetzugang eine andere PPPoE-Sitzung verwenden (anders als ein Host-PC).

Wireless LAN – Falls Sie dieses Kästchen markieren, können PCs im gleichen Wireless-Netzwerk für den Internetzugang eine andere PPPoE-Sitzung verwenden (anders als ein Host-PC).

ISDN-Backup für eine alternative Einwahl - Diese Einstellung ist nur für Router verfügbar, welche die ISDN-Funktion unterstützen. Bevor Sie die ISDN-Backup-Funktion für alternative Einwahl nutzen können, müssen Sie ein Backup-Profil für die Einwahl erstellen. Klicken Sie bitte auf **Einwahl über einen ISP**, um ein Backup-Profil zu erstellen.

Hinweis: - Diese Funktion ist nur für den Port ISDN 2 verfügbar.

Aus - Backup-Funktion deaktivieren.

Automatisch - Die Backup-Leitung wird erst aktiviert, wenn ein Paket vom lokalen Host den Aufbau einer Verbindung durch den Router anstößt.

Immer in Betrieb - Sollte die Breitbandverbindung einmal ausfallen, so wird

die Backup-Leitung automatisch aktiviert und bleibt in Betrieb, bis die Breitbandverbindung wiederhergestellt wird. Verwenden Sie diese Option, falls Sie einen Web-Server betreiben, der für Ihre Kunden ständig erreichbar sein muss.

WAN-Erkennung - Mit dieser Funktion können Sie über ARP oder Ping prüfen, ob Ihre Netzwerkverbindung aktiv ist.

Modus – Wählen Sie zur Überprüfung der WAN-Verbindung durch das System **ARP** oder **Ping**.

Ping IP – Falls Sie als Prüfmodus **Ping** wählen, geben Sie die IP-Adresse in diesem Feld ein.

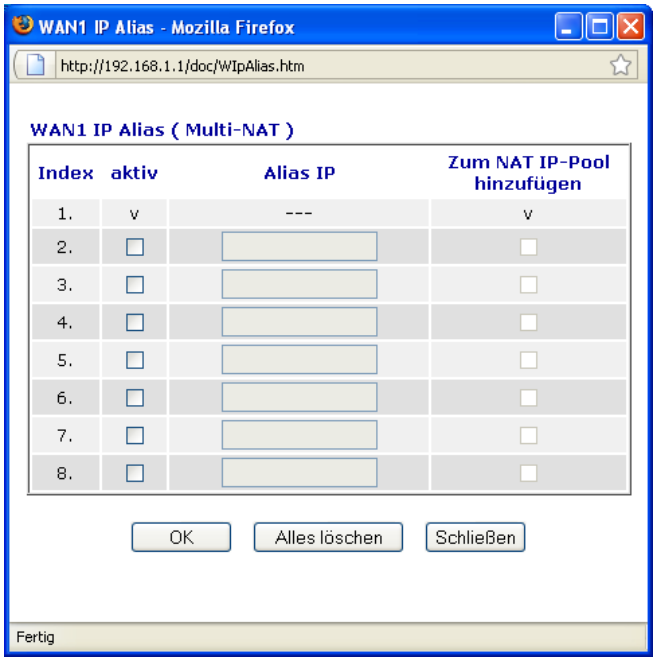
TTL (Time to Live) – Zeigt den vom telnet-Befehl gesetzten TTL-Wert an.

ISP-Einstellungen - Geben Sie den von Ihrem ISP mitgeteilten Benutzernamen, das Passwort und sonstige Authentisierungsparameter ein. Falls Sie ständig mit dem Internet verbunden sein möchten, wählen Sie **Immer in Betrieb**.

Benutzername – Geben Sie den vom ISP mitgeteilten Benutzernamen in diesem Feld ein.

Passwort – Geben Sie das vom ISP mitgeteilte Passwort in diesem Feld ein.

PPP-Authentifizierung – Wählen Sie für PPP entweder **Nur PAP** oder **PAP oder CHAP**.



Max. Leerlaufzeit – Stellen Sie die Leerlaufzeit ein, nach der die Internet-Verbindung abgebrochen werden soll. Diese Einstellung ist nur aktiv, wenn die Betriebsart **Aktiv nach Bedarf** unter **WAN>> Basiskonfiguration** gewählt ist.

IP-Adresse vom ISP - Normalerweise weist der ISP Ihnen dynamisch IP-Adressen zu, wenn Sie sich verbinden und eine Anforderung senden. Einige ISPs bieten einen Service, wobei Sie bei jeder Anforderung die gleiche IP-Adresse zugewiesen bekommen können. In diesem Fall können Sie diese IP-Adresse im Feld **Feste IP** eintragen. Bitte wenden Sie sich an Ihren ISP, bevor Sie diese Funktion verwenden.

WAN-IP Alias - Falls Sie mehrere öffentliche IP-Adressen haben und diese an der WAN-Schnittstelle verwenden möchten, benutzen Sie bitte WAN-IP Alias. Sie können außer der aktuell verwendeten IP-Adresse bis zu acht öffentliche IP-Adressen einrichten. Bitte beachten Sie, dass diese Option lediglich für WAN1 verfügbar ist. Geben Sie die zusätzliche WAN IP-Adresse ein und markieren Sie das Kästchen Aktiv. Dann klicken Sie auf OK, um den Dialog zu verlassen.

Feste IP – Klicken Sie auf **Ja**, um diese Funktion zu nutzen, und geben Sie im Feld **Feste IP-Adresse** eine feste IP-Adresse ein.

Standard-MAC-Adresse – Sie können entweder die **Standard-MAC-Adresse** verwenden oder im entsprechenden Feld eine andere MAC-Adresse für den Router angeben.

MAC-Adresse selbst definieren – Geben Sie die MAC-Adresse für den Router manuell ein.

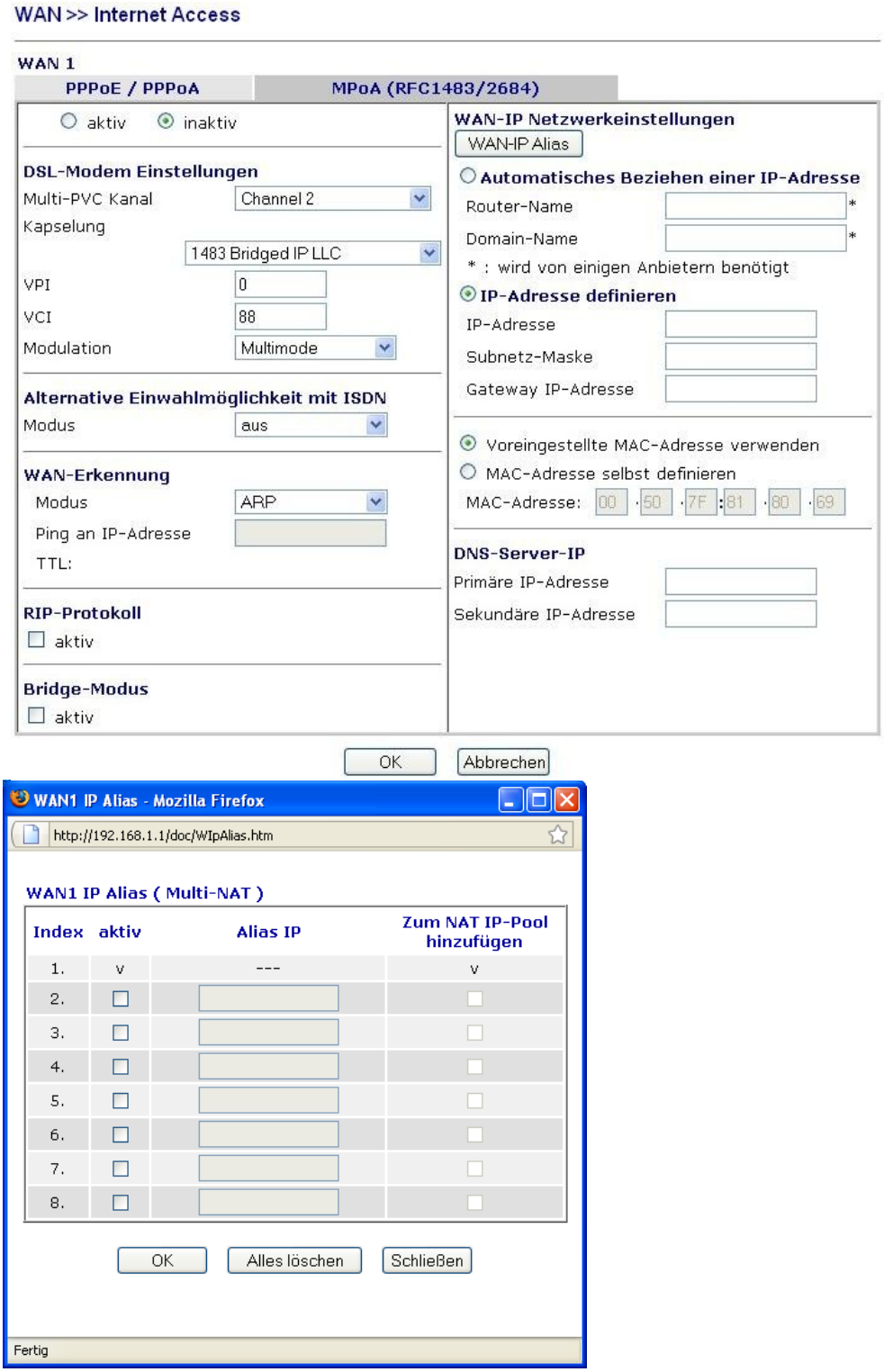
Index (1-15) aus dem Verbindungstimer Konfiguration - Sie können für Ihre Anforderungen vier Verbindungstimer einrichten. Alle Verbindungstimer können im Voraus im Dialog **Anwendungen – Verbindungstimer** eingestellt werden, und Sie können die Nummer verwenden, die Sie in jenem Dialog gesetzt haben.

Nach Abschluss aller Einstellungen klicken Sie auf **OK**, um diese zu aktivieren.

MPoA für WAN1

MPoA ist eine Spezifikation, welche die Integration von ATM-Diensten in bestehenden LANs ermöglicht, die als Protokoll entweder Ethernet, Token Ring, oder TCP/IP verwenden. Das Ziel von MPoA ist, verschiedene LANs zu befähigen, einander über ein ATM-Backbone Pakete zu senden.

Um **MPoA** als das Zugriffsprotokoll des Internets zu verwenden, wählen Sie den **MPoA**-Modus. Der folgende Dialog erscheint:



DSL-Modemeinstellungen - Konfigurieren Sie die für Ihren ISP erforderlichen DSL-Parameter. Diese sind unerlässlich, um zu Ihrem ISP eine DSL-Verbindung aufzubauen.

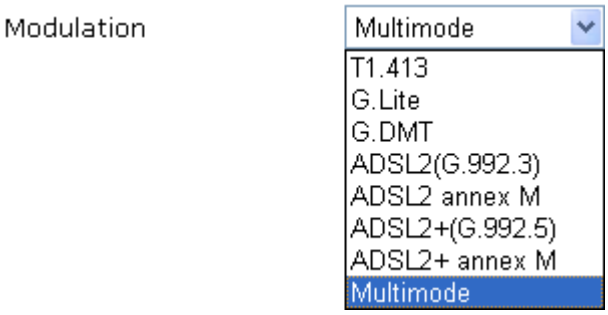
Multi-PVC-Kanal - Die hier angezeigte Auswahl wird von der Seite **Einwahl ins Internet – Multi PVC** bestimmt. **M-PVC-Kanal auswählen** bedeutet, dass keine Auswahl markiert wird.

Kapselung - Dropdown-Liste zur Auswahl des vom ISP bestimmten Typs.

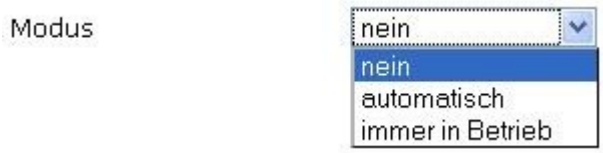
VPI - Geben Sie den vom ISP mitgeteilten Wert ein.

VCI - Geben Sie den vom ISP mitgeteilten Wert ein.

Modulation – Die Standardeinstellung ist **Multimode**. Wählen Sie die Einstellung, die Ihren Bedürfnissen entspricht.



ISDN-Backup für eine alternative Einwahl - Diese Einstellung ist nur für Router verfügbar, welche die ISDN-Funktion unterstützen. Bevor Sie die ISDN-Backup-Funktion für alternative Einwahl nutzen können, müssen Sie ein Backup-Profil für die Einwahl erstellen. Klicken Sie bitte auf **Einwahl über einen ISP**, um ein Backup-Profil zu erstellen.



Hinweis: - Diese Funktion ist nur für den Port ISDN 2 verfügbar.

Aus - Backup-Funktion deaktivieren.

Automatisch - Die Backup-Leitung wird erst aktiviert, wenn ein Paket vom lokalen Host den Aufbau einer Verbindung durch den Router anstößt.

Immer in Betrieb - Sollte die Breitbandverbindung einmal ausfallen, so wird die Backup-Leitung automatisch aktiviert und bleibt in Betrieb, bis die Breitbandverbindung wiederhergestellt wird. Verwenden Sie diese Option, falls Sie einen Web-Server betreiben, der für Ihre Kunden ständig erreichbar sein muss.

WAN-Erkennung - Mit dieser Funktion können Sie über ARP oder Ping prüfen, ob Ihre Netzwerkverbindung aktiv ist.

Modus – Wählen Sie zur Überprüfung der WAN-Verbindung durch das System **ARP** oder **Ping**.

Ping IP – Falls Sie als Prüfmodus **Ping** wählen, geben Sie die IP-Adresse in diesem Feld ein.

TTL (Time to Live) – Zeigt den vom telnet-Befehl

gesetzten TTL-Wert an.

RIP-Protokoll - RIP ist die Abkürzung für Routing Information Protocol (RFC1058), welches bestimmt, wie Router Routing-Tabelleninformationen austauschen. Klicken Sie auf **Aktiv**, um diese Funktion zu aktivieren.

Bridge-Modus - Falls Sie **Bridged IP** als Protokoll wählen, können Sie dieses Kästchen markieren, um die Funktion aufzurufen. Der Router wird als Bridge-Modem laufen.

WAN-IP-Netzwerkeinstellungen - Dieses Menü ermöglicht Ihnen, eine IP-Adresse automatisch zu beziehen oder manuell einzugeben.

Automatisches Beziehen einer IP-Adresse – Klicken Sie auf diese Taste, um die IP-Adresse automatisch zu beziehen.

Router-Name – Geben Sie den vom ISP mitgeteilten Router-Namen ein.

Domain-Name – Geben Sie den zugewiesenen Domain-Namen ein.

IP-Adresse definieren – Klicken Sie auf diese Taste, um einige Daten einzugeben.

WAN-IP Alias - Falls Sie mehrere öffentliche IP-Adressen haben und diese an der WAN-Schnittstelle verwenden möchten, benutzen Sie bitte WAN-IP Alias. Sie können außer der aktuell verwendeten IP-Adresse bis zu acht öffentliche IP-Adressen einrichten. Bitte beachten Sie, dass diese Option lediglich für WAN1 verfügbar ist. Geben Sie die zusätzliche WAN IP-Adresse ein und markieren Sie das Kästchen Aktiv. Dann klicken Sie auf OK, um den Dialog zu verlassen.

IP-Adresse – Geben Sie die private IP-Adresse ein.

Subnetz-Maske – Geben Sie die Subnetz-Maske ein.

Gateway-IP-Adresse – Geben Sie die IP-Adresse des Gateways ein.

Standard-MAC-Adresse - Geben Sie die MAC-Adresse für den Router ein. Sie können entweder die **Standard-MAC-Adresse** verwenden oder bei Bedarf eine andere MAC-Adresse angeben.

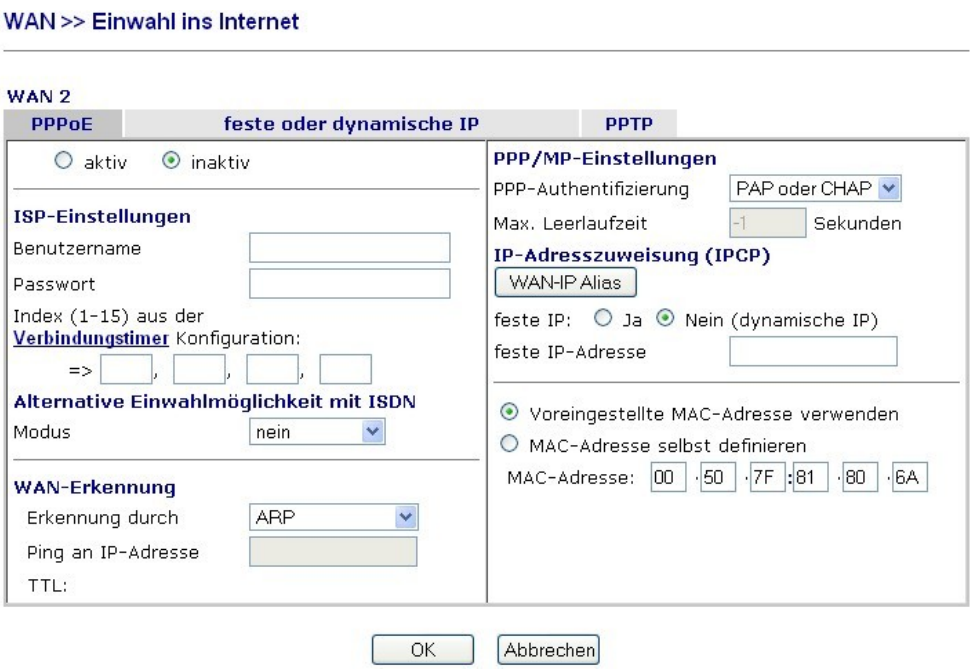
MAC-Adresse – Geben Sie die MAC-Adresse für den Router manuell ein.

DNS-Server-IP - Geben Sie die bevorzugte IP-Adresse für den Router ein. Falls erforderlich, geben Sie eine alternative IP-Adresse ein.

Nach Abschluss aller Einstellungen klicken Sie auf **OK**, um diese zu aktivieren.

PPPoE für WAN2

Um **PPPoE** als das Zugriffsprotokoll des Internets zu verwenden, wählen Sie den **PPPoE**-Modus. Der folgende Dialog erscheint:



Aktiv/Inaktiv - Klicken Sie auf **Aktiv**, um diese Funktion zu aktivieren. Klicken Sie auf **Inaktiv**, so wird diese Funktion geschlossen, und alle auf dieser Seite vorgenommenen Einstellungen werden verworfen.

ISP-Einstellungen - Geben Sie den von Ihrem ISP mitgeteilten Benutzernamen, das Passwort und sonstige Authentisierungsparameter ein. Falls Sie ständig mit dem Internet verbunden sein möchten, wählen Sie **Immer in Betrieb**.

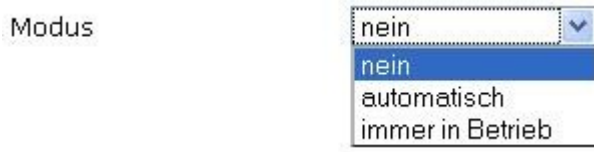
Benutzername – Geben Sie den vom ISP mitgeteilten Benutzernamen in diesem Feld ein.

Passwort – Geben Sie das vom ISP mitgeteilte Passwort in diesem Feld ein.

Index (1-15) aus der Verbindungstimer-Konfiguration - Sie können für Ihre Anforderungen vier Verbindungstimer einrichten. Alle Verbindungstimer können im Voraus im Dialog **Anwendungen – Verbindungstimer** eingestellt werden, und Sie können die Nummer verwenden, die Sie in jenem Dialog gesetzt haben.

ISDN-Backup für eine alternative Einwahl - Diese Einstellung ist nur für Router verfügbar, welche die ISDN-Funktion unterstützen. Bevor Sie die ISDN-Backup-Funktion für alternative Einwahl nutzen können, müssen Sie ein Backup-Profil für die Einwahl erstellen. Klicken Sie bitte

auf **Einwahl über einen ISP**, um ein Backup-Profil zu erstellen.



Hinweis: - Diese Funktion ist nur für den Port ISDN 2 verfügbar.

Aus - Backup-Funktion deaktivieren.

Automatisch - Die Backup-Leitung wird erst aktiviert, wenn ein Paket vom lokalen Host den Aufbau einer Verbindung durch den Router anstößt.

WAN-Erkennung - Mit dieser Funktion können Sie über ARP oder Ping prüfen, ob Ihre Netzwerkverbindung aktiv ist.

Modus – Wählen Sie zur Überprüfung der WAN-Verbindung durch das System **ARP** oder **Ping**.

Ping IP – Falls Sie als Prüfmodus **Ping** wählen, geben Sie die IP-Adresse in diesem Feld ein.

TTL (Time to Live) – Zeigt den vom telnet-Befehl gesetzten TTL-Wert an.

PPP/MP-EinstellungenPPP-Authentifizierung – Wählen Sie für PPP entweder **Nur PAP** oder **PAP oder CHAP**.

Max. Leerlaufzeit – Stellen Sie die Leerlaufzeit ein, nach der die Internet-Verbindung abgebrochen werden soll. Diese Einstellung ist nur aktiv, wenn die Betriebsart **Aktiv nach Bedarf** unter **WAN>> Basiskonfiguration** gewählt ist.

IP-Adresszuweisung (IPCP) - Normalerweise weist der ISP Ihnen dynamisch IP-Adressen zu, wenn Sie sich verbinden und eine Anforderung senden. Einige ISPs bieten einen Service, wobei Sie bei jeder Anforderung die gleiche IP-Adresse zugewiesen bekommen können. In diesem Fall können Sie diese IP-Adresse im Feld Feste IP eintragen. Bitte wenden Sie sich an Ihren ISP, bevor Sie diese Funktion verwenden.

WAN-IP Alias - Falls Sie mehrere öffentliche IP-Adressen haben und diese an der WAN-Schnittstelle verwenden möchten, benutzen Sie bitte WAN-IP Alias. Sie können außer der aktuell verwendeten IP-Adresse bis zu acht öffentliche IP-Adressen einrichten. Bitte beachten Sie, dass diese Option lediglich für WAN1 verfügbar ist. Geben Sie die zusätzliche WAN IP-Adresse ein und markieren Sie das

Kästchen Aktiv. Dann klicken Sie auf OK, um den Dialog zu verlassen.

Feste IP – Klicken Sie auf **Ja**, um diese Funktion zu nutzen, und geben Sie im Feld **Feste IP-Adresse** eine feste IP-Adresse ein.

Feste IP-Adresse -Geben Sie eine feste IP-Adresse ein.

Standard-MAC-Adresse– Sie können entweder die **Standard-MAC-Adresse** verwenden oder im entsprechenden Feld eine andere MAC-Adresse für den Router angeben.

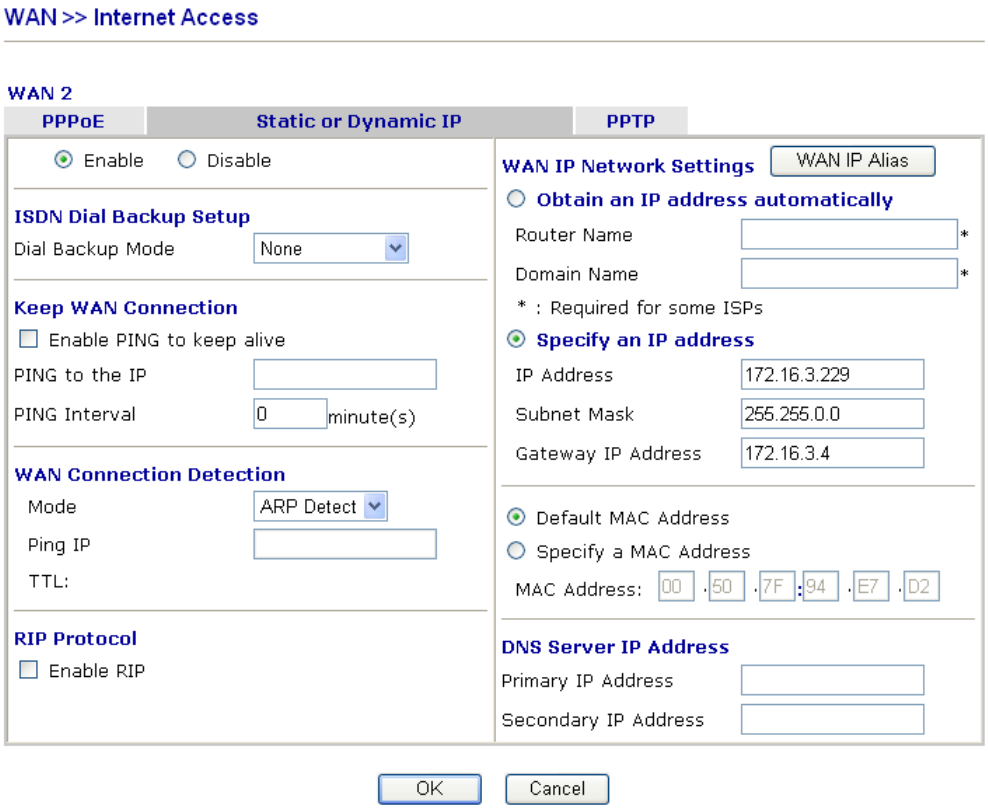
MAC-Adresse selbst definieren – Geben Sie die MAC-Adresse für den Router manuell ein.

Nach Abschluss aller Einstellungen klicken Sie auf **OK**, um diese zu aktivieren.

Feste oder dynamische IP für WAN2

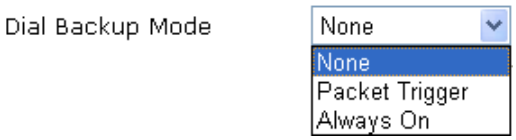
Für den festen IP-Modus erhalten Sie meistens von Ihrem DSL- oder Kabel-ISP eine öffentliche IP-Adresse. Falls Sie ein öffentliches Subnetz von Ihrem ISP erhalten haben, können Sie der WAN-Schnittstelle eine oder mehrere IP-Adressen zuweisen.

Um eine feste oder dynamische IP als Zugriffsprotokoll für das Internet zu verwenden, wählen Sie als Modus **Feste oder Dynamische IP**. Der folgende Dialog erscheint:



Aktiv/Inaktiv - Klicken Sie auf **Aktiv**, um diese Funktion zu aktivieren. Klicken Sie auf **Inaktiv**, so wird diese Funktion geschlossen, und alle auf dieser Seite vorgenommenen Einstellungen werden verworfen.

ISDN-Backup für eine alternative Einwahl - Diese Einstellung ist nur für Router verfügbar, welche die ISDN-Funktion unterstützen. Bevor Sie die ISDN-Backup-Funktion für alternative Einwahl nutzen können, müssen Sie ein Backup-Profil für die Einwahl erstellen. Klicken Sie bitte auf **Einwahl über einen ISP**, um ein Backup-Profil zu erstellen.



Hinweis: - Diese Funktion ist nur für den Port ISDN 2 verfügbar.

Aus - Backup-Funktion deaktivieren.

Automatisch - Die Backup-Leitung wird erst aktiviert, wenn ein Paket vom lokalen Host den Aufbau einer Verbindung durch den Router anstößt.

Immer in Betrieb - Sollte die Breitbandverbindung einmal ausfallen, so wird die Backup-Leitung automatisch aktiviert und bleibt in Betrieb, bis die Breitbandverbindung wiederhergestellt wird. Verwenden Sie diese Option, falls Sie einen Web-Server betreiben, der für Ihre Kunden ständig erreichbar sein muss.

WAN-Erkennung - Mit dieser Funktion können Sie über ARP oder Ping prüfen, ob Ihre Netzwerkverbindung aktiv ist.

Modus – Wählen Sie zur Überprüfung der WAN-Verbindung durch das System **ARP** oder **Ping**.

Ping IP – Falls Sie als Prüfmodus **Ping** wählen, geben Sie die IP-Adresse in diesem Feld ein.

TTL (Time to Live) – Zeigt den vom telnet-Befehl gesetzten TTL-Wert an.

Abbruch der Internetverbindung vermeiden - Diese Funktion ist für dynamische IP-Umgebungen nützlich, da einige ISPs die Verbindung abbrechen, falls innerhalb eines bestimmten Zeitraums kein Verkehr aufkommt. Markieren Sie das Kästchen **Dauer-Ping aktiv**, um diese Funktion zu aktivieren.

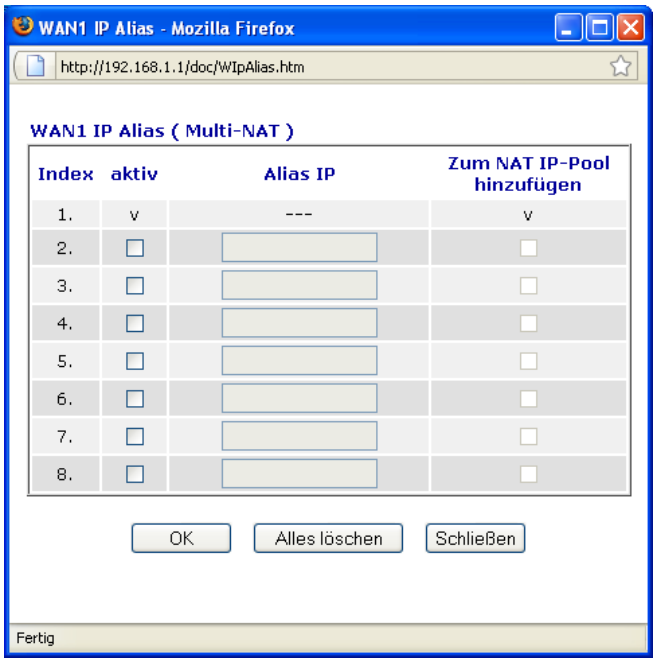
Ping an die IP - Um die Ping-Funktion zu verwenden, um die Verbindung aufrechtzuerhalten, geben Sie bitte die IP-Adresse ein.

Ping-Intervall - Geben Sie das Intervall für die Ausführung des Ping-Befehls ein.

RIP-Protokoll - RIP ist die Abkürzung für Routing Information Protocol (RFC1058), welches bestimmt, wie Router Routing-Tabelleninformationen austauschen. Klicken Sie auf **Aktiv**, um diese Funktion zu aktivieren.

WAN-IP-Netzwerkeinstellungen - Dieses Menü ermöglicht Ihnen, eine IP-Adresse automatisch zu beziehen oder manuell einzugeben.

WAN-IP Alias - Falls Sie mehrere öffentliche IP-Adressen haben und diese an der WAN-Schnittstelle verwenden möchten, benutzen Sie bitte WAN-IP Alias. Sie können außer der aktuell verwendeten IP-Adresse bis zu acht öffentliche IP-Adressen einrichten. Bitte beachten Sie, dass diese Option lediglich für WAN1 verfügbar ist. Geben Sie die zusätzliche WAN IP-Adresse ein und markieren Sie das Kästchen Aktiv. Dann klicken Sie auf OK, um den Dialog zu verlassen.



Automatisches Beziehen einer IP-Adresse – Klicken Sie auf diese Taste, um im Modus **Dynamische IP** die IP-Adresse automatisch zu beziehen.

Router-Name: - Geben Sie den vom ISP mitgeteilten Router-Namen ein.

Domain-Name: - Geben Sie den zugewiesenen Domain-Namen ein.

IP-Adresse definieren – Klicken Sie auf diese Taste, um im Modus **Feste IP** eine Reihe von Daten einzugeben.

IP-Adresse: - Geben Sie die IP-Adresse ein.

***Subnetz-Maske**:* - Geben Sie die Subnetz-Maske ein.

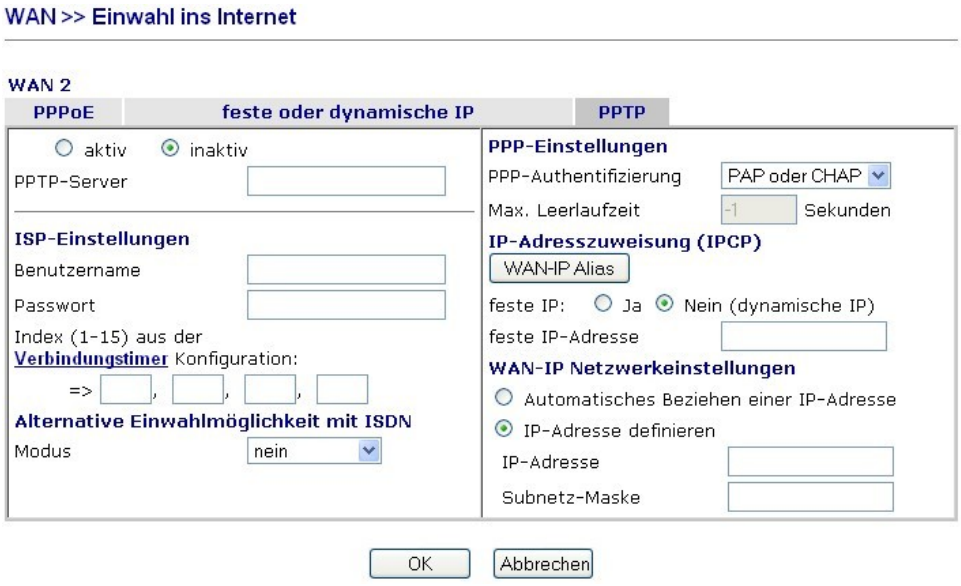
***Gateway-IP-Adresse**:* - Geben Sie die IP-Adresse des Gateways ein.

Voreingestellte MAC-Adresse verwenden: - Klicken Sie auf diese Schaltfläche, um für den Router die voreingestellte MAC-Adresse zu verwenden.

MAC-Adresse selbst definieren: - Einige Kabeldienstleister stellen für die Zugriffsautenthifizierung eine bestimmte MAC-Adresse zur Verfügung. In diesem Fall klicken Sie auf **MAC-Adresse selbst definieren** und geben die MAC-Adresse im entsprechenden Feld ein.

DNS-Server-IP - Geben Sie für den Modus **Feste IP** die primäre IP-Adresse ein. Falls erforderlich, geben Sie eine alternative IP-Adresse ein.

Um **PPTP/L2TP -** als das Zugriffsprotokoll des Internets zu verwenden, wählen Sie den **PPTP/L2TP**-Modus. Der folgende Dialog erscheint:



Aktiv/Inaktiv - Klicken Sie auf **Aktiv**, um diese Funktion zu aktivieren. Klicken Sie auf **Inaktiv**, so wird diese Funktion geschlossen, und alle auf dieser Seite vorgenommenen Einstellungen werden verworfen.

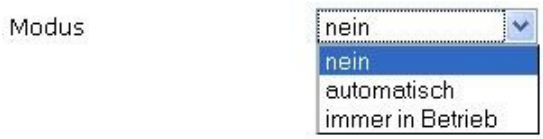
PPTP-Server - Geben Sie die IP-Adresse des PPTP-Servers an.

ISP-EinstellungenBenutzername - Geben Sie den vom ISP mitgeteilten Benutzernamen in diesem Feld ein.

Passwort - Geben Sie das vom ISP mitgeteilte Passwort in diesem Feld ein.

Index (1-15) aus der Verbindungstimer-Konfiguration - Sie können für Ihre Anforderungen vier Verbindungstimer einrichten. Alle Verbindungstimer können im Voraus im Dialog **Anwendungen – Verbindungstimer** eingestellt werden, und Sie können die Nummer verwenden, die Sie in jenem Dialog gesetzt haben.

ISDN-Backup für eine alternative Einwahl - Diese Einstellung ist nur für Router verfügbar, welche die ISDN-Funktion unterstützen. Bevor Sie die ISDN-Backup-Funktion für alternative Einwahl nutzen können, müssen Sie ein Backup-Profil für die Einwahl erstellen. Klicken Sie bitte auf **Einwahl über einen ISP**, um ein Backup-Profil zu erstellen.



Hinweis: - Diese Funktion ist nur für den Port ISDN 2 verfügbar.

Aus - Backup-Funktion deaktivieren.

Automatisch - Die Backup-Leitung wird erst aktiviert, wenn ein Paket vom lokalen Host den Aufbau einer Verbindung durch den Router anstößt.

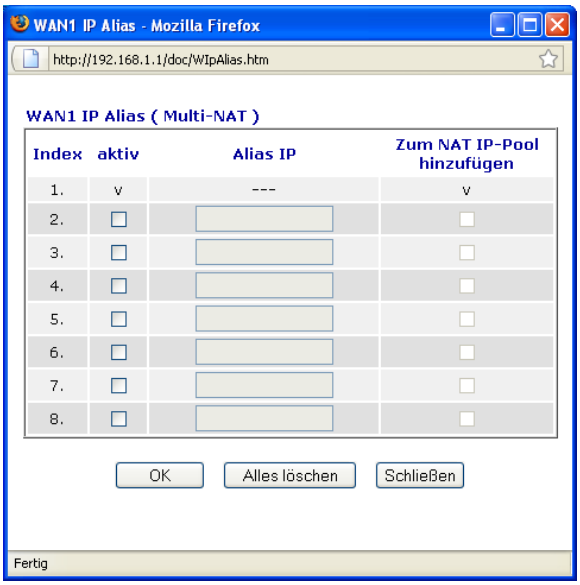
PPP-EinstellungenPPP-Authentifizierung - Wählen Sie für PPP entweder **Nur PAP** oder **PAP oder CHAP**.

Max. Leerlaufzeit - Stellen Sie die Leerlaufzeit ein, nach der die Internet-Verbindung abgebrochen werden soll. Diese Einstellung ist nur aktiv, wenn die Betriebsart **Aktiv nach Bedarf** unter **WAN>> Basiskonfiguration** gewählt ist.

IP-Adresszuweisung (IPCP) - Normalerweise weist der ISP Ihnen dynamisch IP-Adressen zu, wenn Sie sich verbinden und eine Anforderung senden. Einige ISPs bieten einen Service, wobei Sie bei jeder Anforderung die gleiche IP-Adresse zugewiesen bekommen können. In diesem Fall können Sie diese IP-Adresse im Feld **Feste IP** eintragen. Bitte wenden Sie sich an Ihren ISP, bevor Sie diese Funktion verwenden.

WAN-IP Alias - Falls Sie mehrere öffentliche IP-Adressen haben und diese an der WAN-Schnittstelle verwenden möchten, benutzen Sie bitte WAN-IP Alias. Sie können außer der

aktuell verwendeten IP-Adresse bis zu acht öffentliche IP-Adressen einrichten. Bitte beachten Sie, dass diese Option lediglich für WAN1 verfügbar ist. Geben Sie die zusätzliche WAN IP-Adresse ein und markieren Sie das Kästchen Aktiv. Dann klicken Sie auf OK, um den Dialog zu verlassen.



Klicken Sie auf **Ja**, um diese Funktion zu nutzen, und geben Sie im Feld eine feste IP-Adresse ein.

Feste IP - Klicken Sie auf **Ja**, um diese Funktion zu nutzen, und geben Sie im Feld **Feste IP-Adresse** eine feste IP-Adresse ein.

Feste IP-Adresse -Geben Sie eine feste IP-Adresse ein.

WAN-IP-Netzwerkeinstellungen
Automatisches Beziehen einer IP-Adresse – Klicken Sie auf diese Taste, um die IP-Adresse automatisch zu beziehen.

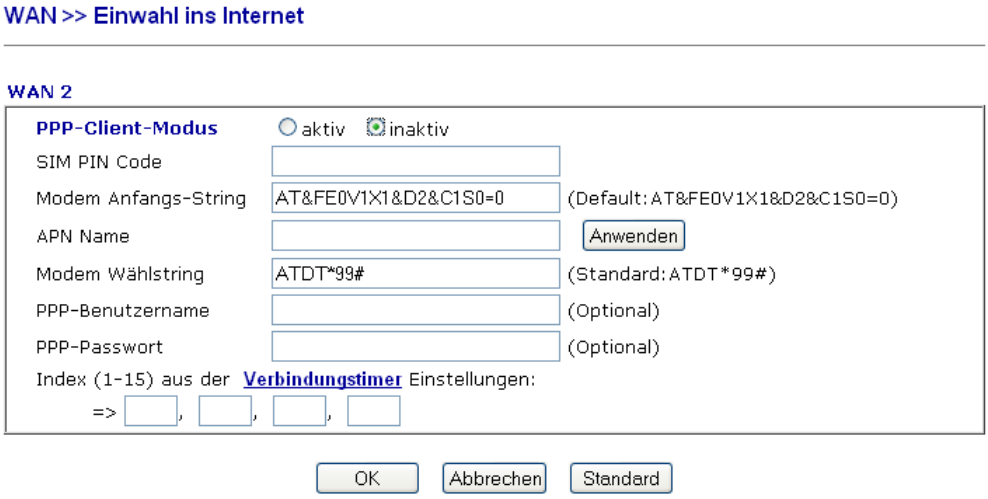
IP-Adresse definieren – Klicken Sie auf diese Taste, um einige Daten einzugeben.

IP-Adresse – Geben Sie die IP-Adresse ein.

Subnetz-Maske – Geben Sie die Subnetz-Maske ein.

PPP für WAN2

Dieser Modus ist nur aktiv, wenn **3G USB-Modem** in der Basiskonfiguration als Modus gewählt wurde.



PPP-Client-Modus - Klicken Sie auf Aktiv, um diesen Modus für WAN2 zu aktivieren.

SIM PIN Code - Geben Sie den PIN-Code der SIM-Karte ein, die Sie zur Einwahl ins Internet verwenden.

Modem Anfangs-String - Dieser Wert wird verwendet, um das USB-Modem zu initialisieren. Bitte benutzen Sie den Standardwert. Eventuell verwendet Ihr ISP einen anderem Wert, bitte wenden Sie sich in diesen Fall an Ihren ISP.

APN Name - Der APN (Access Point Name) wird Ihnen von Ihrem ISP mitgeteilt, um verschiedene Access Points zu identifizieren. Klicken Sie einfach auf **Anwenden**, um einen solchen Namen anzuwenden. Abschließend klicken Sie auf **OK**, um die Einstellung zu speichern.

Anwenden – Identifizierungsfunktion aktivieren.

Modem Wählstring - Dieser Wert wird zum Wählen im USB-Modus verwendet. Bitte benutzen Sie den Standardwert. Sollten Sie hierzu Fragen haben, wenden Sie sich bitte an Ihren ISP.

PPP-Benutzername - Geben Sie den PPP-Benutzernamen ein (optional).

PPP-Passwort - Geben Sie das PPP-Passwort

ein (optional).

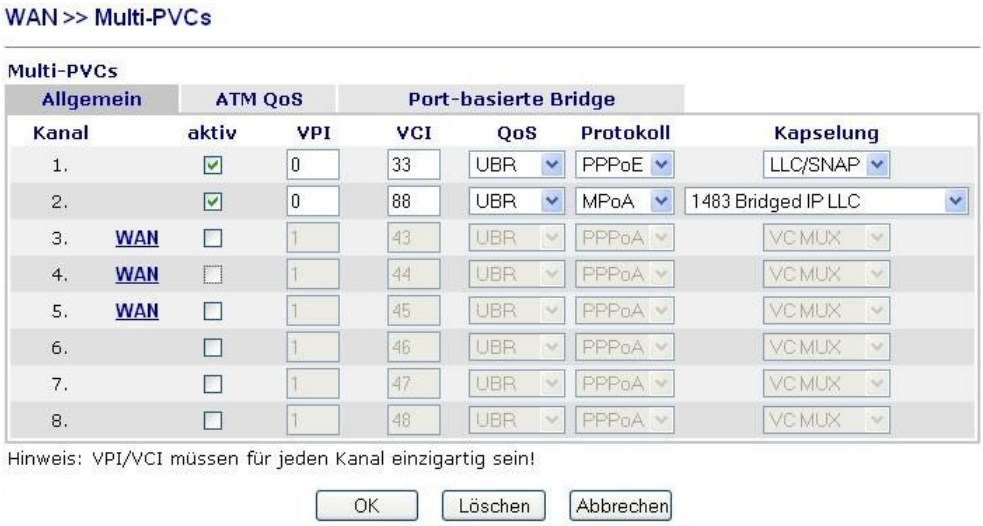
Index (1-15) - Sie können die LAN-PCs so konfigurieren, dass sie lediglich in gewissen Zeitabschnitten in Betrieb sind. Sie können bis zu vier der 15 vordefinierten Timer unter **Anwendungen >> Timer** wählen. Per Standardeinstellung ist dieses Feld leer, und die Funktion ist ständig in Betrieb.

5.1.5 Multi-PVCs

Dieser Router ermöglicht Ihnen die Einrichtung von Multi-PVCs für verschiedene Datenübertragungen. Zur Konfiguration gehen Sie zu **Einwahl ins Internet** und wählen die Seite **Multi-PVC**.

Allgemein

Das System ermöglicht Ihnen, bis zu acht Kanäle, die als erste PVC-Leitung gewählt werden können, als Multi-PVCs zu bestimmen.

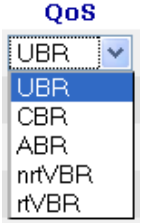


Aktiv - Markieren Sie dieses Kästchen, um den Kanal zu aktivieren. Die hier aktivierten Kanäle werden in der Dropdown-Liste **Multi-PVC-Kanäle** im Dialog **Einwahl ins Internet** angezeigt. Obwohl Sie auf dieser Seite acht Kanäle aktivieren können, kann nur ein Kanal im Dialog **Einwahl ins Internet** gewählt werden.

VPI - Geben Sie den vom ISP mitgeteilten Wert ein.

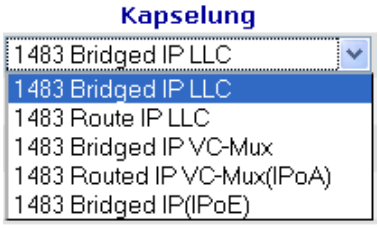
VCI - Geben Sie den vom ISP mitgeteilten Wert ein.

QoS-Typ - Wählen Sie für den Kanal einen geeigneten QoS-Typ.



Protokoll - Wählen Sie ein geeignetes Protokoll für diesen Kanal.

Kapselung - Wählen Sie einen geeigneten Typ für diesen Kanal. Die Typen ändern sich je nach gewählter Protokolleinstellung.



WAN-Verbindungen für die Kanäle 3, 4, 5 werden für Router-eigene Anwendungen wie TR-069 und VoIP bereitgestellt. Die notwendigen Einstellungen erhalten Sie von Ihrem ISP. Bei Bedarf wenden Sie sich bitte an Ihren ISP und klicken dann auf die WAN-Verbindung von Kanal 3, 4 oder 5, um Ihren Router zu konfigurieren.

WAN für Router-eigene Anwendungen - Wählen Sie den Router-Dienst für Kanal 3, 4 oder 5.

Management - Kann für allgemeines Management (Web-Konfiguration/Telnet/TR069) ausgewählt werden. Wenn Sie Management wählen, gilt die Konfiguration dieses PVCs für die Web-Konfiguration/Telnet/TR069.

VoIP - Kann nur für VoIP gewählt werden. Wenn Sie VoIP wählen, gilt die Konfiguration dieses PVCs für die Übertragung und den Empfang von VoIP-Daten.

Aktiv/Inaktiv - Klicken Sie auf **Aktiv**, um diese Funktion zu aktivieren. Klicken Sie auf **Inaktiv**, so wird diese Funktion geschlossen, und alle auf dieser Seite vorgenommenen Einstellungen werden verworfen.

DSL-Modemeinstellungen - Konfigurieren Sie die für Ihren ISP erforderlichen DSL-Parameter. Diese sind erforderlich, um zu Ihrem ISP eine DSL-Verbindung aufzubauen.

VPI - Geben Sie den vom ISP mitgeteilten Wert ein.

VCI - Geben Sie den vom ISP mitgeteilten Wert ein.

QoS-Typ - Wählen Sie für den Kanal einen geeigneten QoS-Typ.

Protokoll - Wählen Sie ein geeignetes Protokoll für diesen Kanal. Sie haben die Wahl zwischen PPPoE, PPPoA und MPoA. Die folgenden Einstellungen unterscheiden sich je nach dem hier gewählten Protokoll.

Kapselung - Dropdown-Liste zur Auswahl des vom ISP bestimmten Typs.

ISP-Einstellungen - Geben Sie den von Ihrem ISP mitgeteilten Benutzernamen, das Passwort und sonstige Authentisierungsparameter ein. Falls Sie ständig mit dem Internet verbunden sein möchten, wählen Sie **Immer in Betrieb**.

Benutzername – Geben Sie den vom ISP mitgeteilten Benutzernamen in diesem Feld ein.

Passwort – Geben Sie das vom ISP mitgeteilte Passwort in diesem Feld ein.

PPP-Authentifizierung – Wählen Sie für PPP entweder **Nur PAP** oder **PAP oder CHAP**.

Max. Leerlaufzeit – Stellen Sie die Leerlaufzeit ein, nach der die Internet-Verbindung abgebrochen werden soll. Diese Einstellung ist nur aktiv, wenn **Immer in Betrieb** nicht ausgewählt ist.

IP-Adresse vom ISPFeste IP – Klicken Sie auf **Ja**, um diese Funktion zu nutzen, und geben Sie im Feld **Feste IP-Adresse** eine feste IP-Adresse ein.

Feste IP-Adresse – Geben Sie eine feste IP-Adresse ein.

Automatisches Beziehen einer IP-Adresse - Klicken Sie auf diese Taste, um die IP-Adresse automatisch zu beziehen.

Router-Name – Geben Sie den vom ISP mitgeteilten Router-Namen ein.

Domain-Name – Geben Sie den zugewiesenen Domain-Namen ein.

IP-Adresse definieren - Klicken Sie auf diese Taste, um IP-Daten einzugeben.

IP-Adresse – Geben Sie die private IP-Adresse ein.

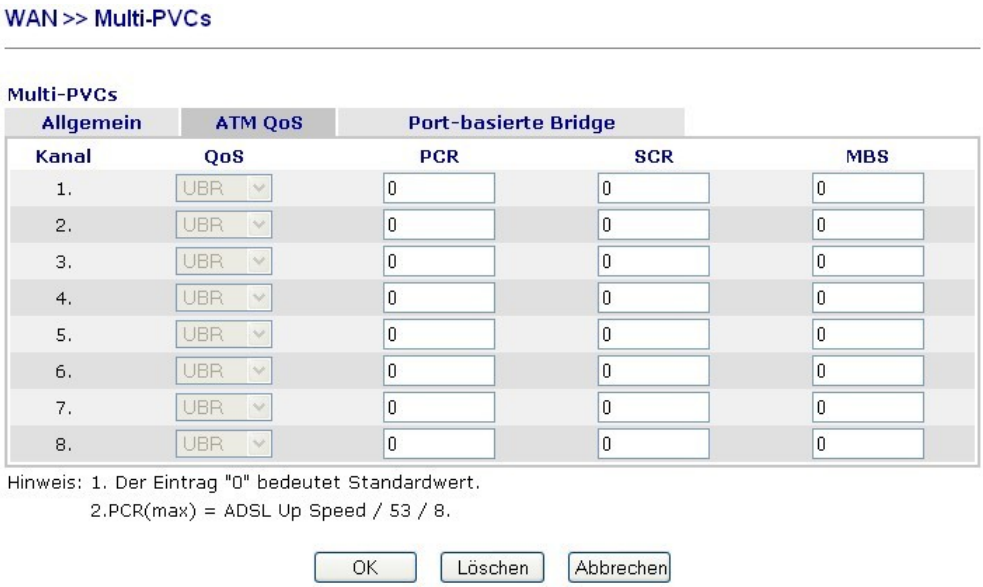
Subnetz-Maske – Geben Sie die Subnetz-Maske ein.

Gateway-IP-Adresse – Geben Sie die IP-Adresse des Gateways ein.

DNS-Server-IP - Geben Sie die bevorzugte IP-Adresse für den Router ein. Falls erforderlich, geben Sie eine alternative IP-Adresse ein.

ATM QoS

Diese Konfiguration bezieht sich auf die Upstream-Pakete. Die Information wird von Ihrem ISP bereitgestellt. Bitte wenden Sie sich für Einzelheiten an Ihren ISP.



QoS-Typ - Wählen Sie für den Kanal einen geeigneten QoS-Typ gemäß der Information von Ihrem ISP.

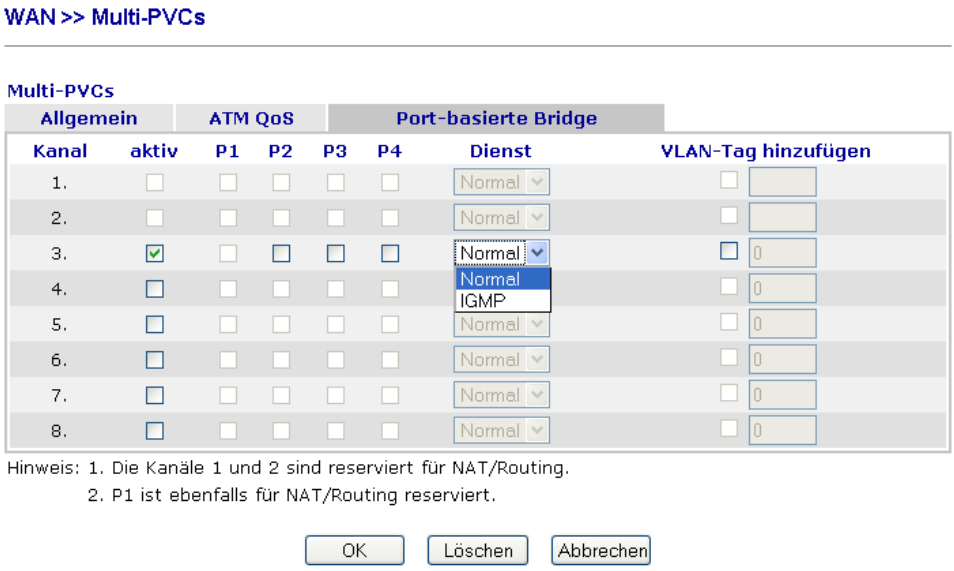
PCR - Abkürzung für Peak Cell Rate. Die Standardeinstellung ist "0".

SCR - Abkürzung für Sustainable Cell Rate. Der SCR-Wert muss kleiner als der PCR-Wert sein.

MBS - Abkürzung für Maximum Burst Size. Der Wertebereich reicht von 10 bis 50.

Port-basierte Brücke

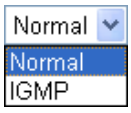
Auf der Seite Allgemein können Sie den ersten PVC einstellen. Zur Einstellung des zweiten PVC klicken Sie bitte auf den Reiter **Port-basierte Brücke**, um die Konfigurationsseite für die Brücke zu öffnen.



Aktiv - Markieren Sie dieses Kästchen, um den Kanal zu aktivieren. Auf dieser Seite können nur die Kanäle 3 bis 8 gesetzt werden, da die Kanäle 1 und 4 für NAT reserviert sind.

P1 bis P4 - Bezieht sich auf die LAN-Ports 1 bis 4. Markieren Sie das Kästchen, um die LAN-Ports für die Kanäle 3 bis 8 festzulegen.

Servicetyp - Normalerweise wird der Servicetyp für den Dienst des Video-Streams verwendet (z.B. IPTV). Er kann die Pakete der Fernsteuerung und des Video-Streams verschiedenen PVCs zuteilen. Meistens wird für die Fernsteuerung das IGMP-Protokoll benutzt.



Normal – Bedeutet, dass PVC alle Pakete außer IGMP annehmen kann.

IGMP – Bedeutet, dass PVC lediglich IGMP-Pakete annehmen kann.

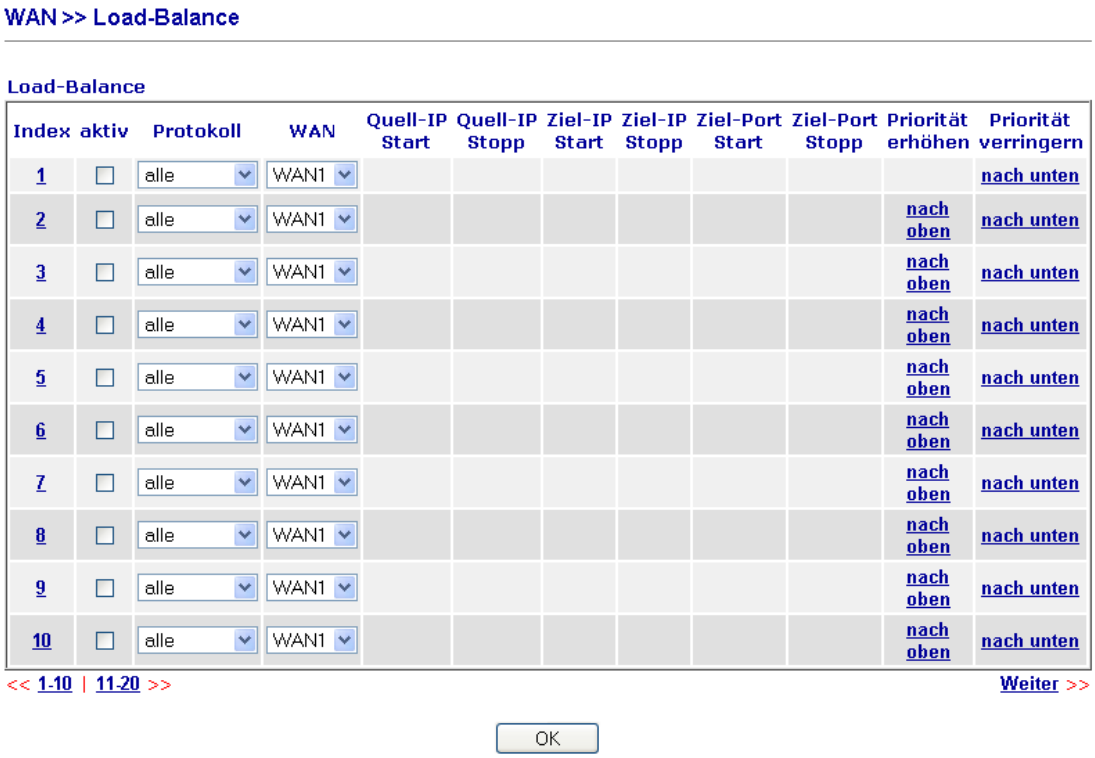
Tag hinzufügen - Um die Verwendung von PVC zu kennzeichnen, markieren Sie dieses Kästchen, um diese Einstellung zu aktivieren. Geben Sie die VLAN ID-Nummer ein.

Klicken Sie auf **Löschen**, um alle Konfigurationen auf dieser Seite zu entfernen, falls Sie mit diesen nicht zufrieden sind. Um die Konfiguration fertig zu stellen, klicken Sie auf **OK**, um die Einstellungen zu sichern und die Seite zu verlassen. Um die Konfiguration abzubrechen und die Seite zu verlassen, klicken Sie auf Abbrechen.

5.1.6 Load-Balance

Dieser Router unterstützt Load-Balance. Load-Balance ermöglicht die Zuweisung des Datenverkehrs zu einem bestimmten Protokolltyp, der IP-Adresse eines spezifischen Hosts oder eines Port-Bereichs zur WAN1- oder WAN2-Schnittstelle. Der Benutzer kann Verkehrskategorien setzen und den Datenverkehr gemäß den Einstellungen im folgenden Dialog über eine dedizierte Netzwerkschnittstelle leiten. Dieser Router unterstützt bis zu 20 Load-Balance-Policies.

Hinweis: Load-Balance funktioniert nur, wenn sowohl WAN1 als auch WAN2 aktiviert ist.


WAN >> Load-Balance
Load-Balance
Index aktiv Protokoll WAN Quell-IP Start Quell-IP Stopp Ziel-IP Start Ziel-IP Stopp Ziel-Port Start Ziel-Port Stopp Priorität erhöhen Priorität verringern
1 alle WAN1 nach unten
2 alle WAN1 nach oben nach unten
3 alle WAN1 nach oben nach unten
4 alle WAN1 nach oben nach unten
5 alle WAN1 nach oben nach unten
6 alle WAN1 nach oben nach unten
7 alle WAN1 nach oben nach unten
8 alle WAN1 nach oben nach unten
9 alle WAN1 nach oben nach unten
10 alle WAN1 nach oben nach unten
<< 1-10 | 11-20 >>
Weiter >>
OK

Index - Klicken Sie auf die entsprechende Indexnummer, um auf die Seite zu gelangen, auf der Sie die Load-Balance-Einstellungen konfigurieren können.

Aktiv - Markieren Sie dieses Kästchen, um diese Funktion zu aktivieren.

Protokoll - Verwenden Sie das Dropdown-Menü, um das Protokoll für die WAN-Schnittstelle zu ändern.

WAN - Verwenden Sie das Dropdown-Menü, um die WAN-Schnittstelle zu ändern.

Quell-IP Start - Zeigt die erste Quell-IP an.

Quell-IP Stopp - Zeigt die letzte Quell-IP an.

Ziel-IP Start - Zeigt die erste Ziel-IP an.

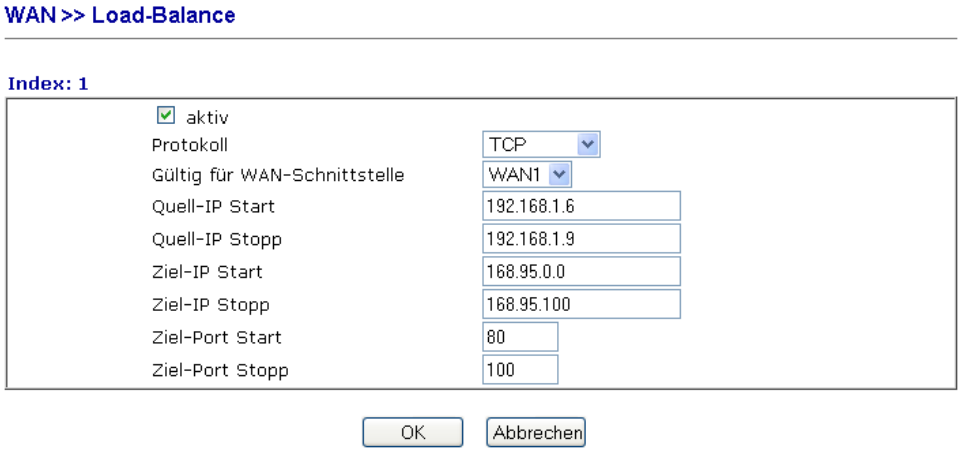
Ziel-IP Stopp - Zeigt die letzte Ziel-IP an.

Ziel-Port Start - Zeigt den ersten Ziel-Port an.

Ziel-Port Stopp - Zeigt den letzten Ziel-Port an.

Aufwerten/Abwerten - Klicken Sie auf **Nach oben** oder **Nach unten**, um die Reihenfolge der Policy zu ändern.

Klicken Sie auf **Index 1**, um auf die folgende Seite zu gelangen, auf der Sie die Load-Balance-Einstellungen konfigurieren können.



Aktiv - Markieren Sie dieses Kästchen, um diese Funktion zu aktivieren.

Protokoll - Verwenden Sie das Dropdown-Menü, um das richtige Protokoll für die WAN-Schnittstelle zu wählen.

Gültig für WAN-Schnittstelle - Wählen Sie die WAN-Schnittstelle (WAN1 oder WAN2) für die Bindung.

Quell-IP Start - Geben Sie die erste Quell-IP für die angegebene Schnittstelle ein.

Quell-IP Stopp - Geben Sie die letzte Quell-IP für die angegebene Schnittstelle ein. Falls dieses Feld leer gelassen wird, werden alle Quell-IPs im LAN durch die WAN-Schnittstelle geleitet.

Ziel-IP Start - Geben Sie die erste Ziel-IP für die angegebene Schnittstelle ein.

Ziel-IP Stopp - Geben Sie die letzte Ziel-IP für die angegebene Schnittstelle ein. Falls dieses Feld leer gelassen wird, werden alle Ziel-IPs durch die WAN-Schnittstelle geleitet.

Ziel-Port Start - Geben Sie den ersten Ziel-Port für den Ziel-IP-Bereich ein.

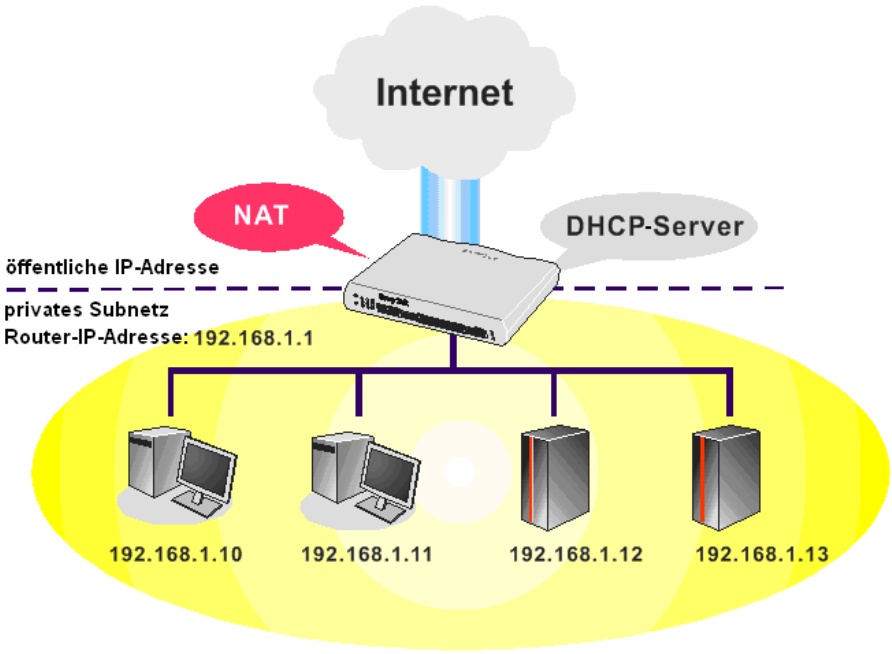
Ziel-Port Stopp - Geben Sie den letzten Ziel-Port für den Ziel-IP-Bereich ein. Falls dieses Feld leer gelassen wird, werden alle Ziel-Ports durch die WAN-Schnittstelle geleitet.

5.2 LAN

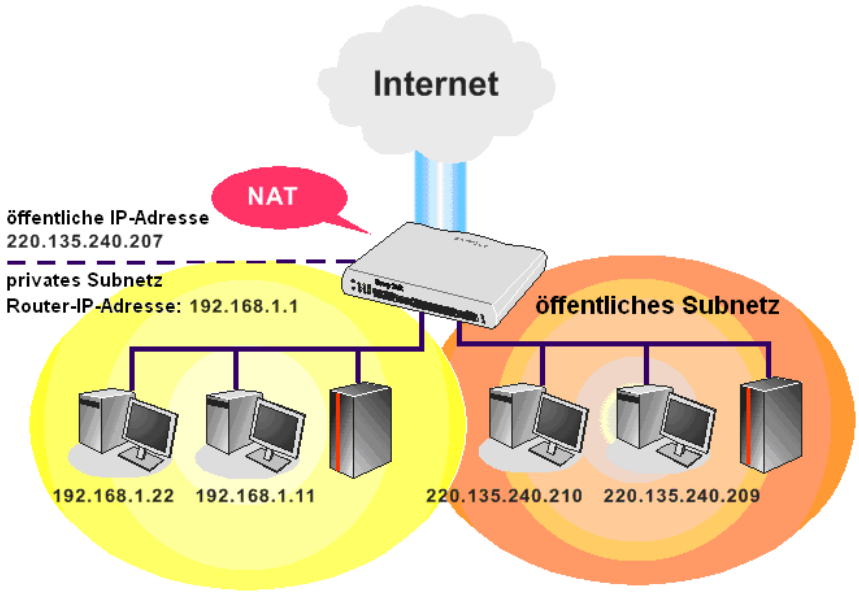
Das Local Area Network (LAN) ist eine Gruppe von Subnetzen, die vom Router verwaltet und gesteuert werden. Die Netzwerkstruktur hängt davon ab, welche Art von öffentlichen IP-Adressen Ihnen Ihr ISP zuweist.

5.2.1 LAN-Grundlagen

Die grundlegende Funktion des Vigor-Routers ist NAT. Hiermit wird ein privates Subnetz aufgebaut. Wie bereits erwähnt, kommuniziert der Router über die öffentliche IP-Adresse mit anderen öffentlichen Hosts im Internet und über die private IP-Adresse mit lokalen Hosts. NAT hat die Aufgabe, die Pakete von der öffentlichen IP-Adresse auf private IP-Adressen umzuschreiben und die entsprechenden Pakete zum richtigen Host und umgekehrt weiterzuleiten. Außerdem verfügt der Vigor-Router über einen eingebauten DHCP-Server, der jedem lokalen Host private IP-Adressen zuweist. Die folgende Abbildung dient dem besseren Verständnis:



In einigen Sonderfällen können Sie von Ihrem ISP ein öffentliches IP-Subnetz wie 220.135.240.0/24 erhalten. Dies bedeutet, dass Sie ein öffentliches Subnetz einrichten können oder ein zweites Subnetz bestimmen können, in dem jeder Host eine öffentliche IP-Adresse erhält. Als Teil des öffentlichen Subnetzes ist der Vigor-Router für das IP-Routing verantwortlich, um Hosts im öffentlichen Subnetz zu ermöglichen, mit anderen öffentlichen Hosts oder Servern zu kommunizieren, die außerhalb liegen. Deswegen sollte der Router als Gateway für öffentliche Hosts eingerichtet werden.



Was ist das Routing Information Protocol (RIP)?

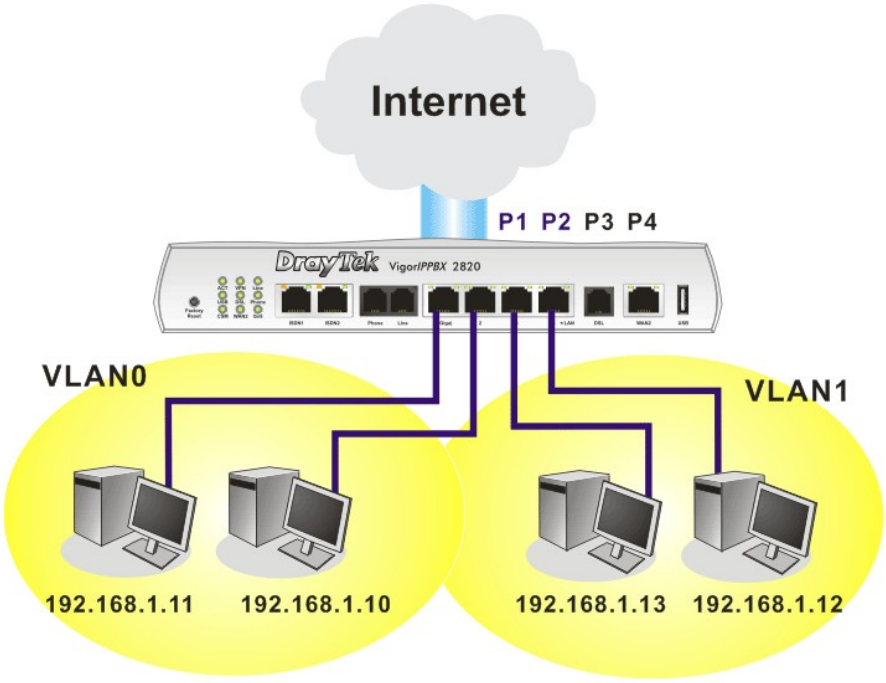
Der Vigor-Router tauscht mit Hilfe von RIP Routing-Informationen mit benachbarten Routern aus, um IP-Routing zu ermöglichen. Auf diese Weise benachrichtigen sich die Router automatisch, wenn Benutzer Daten des Routers ändern, z.B. die IP-Adresse.

Was ist eine feste Adressumleitung?

Falls Sie in Ihrem LAN mehrere Subnetze haben, sind **feste Adressumleitungen** die schnellste und effektivste Möglichkeit, Verbindungen herzustellen. Sie können einfach Regeln für die Weiterleitung von Daten aus einem angegebenen Subnetz in ein anderes angegebenes Subnetz festlegen, ohne RIP zu verwenden.

Was sind virtuelle LANs?

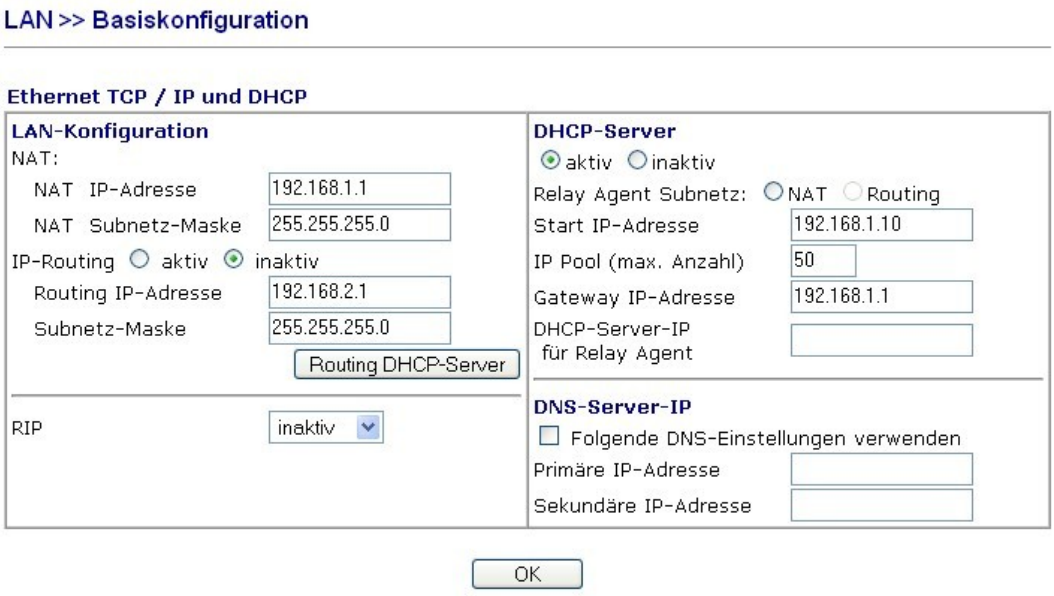
Sie können lokale Hosts nach physischen Ports gruppieren und bis zu vier virtuelle LANs einrichten. Um die Kommunikation zwischen verschiedenen Gruppen zu verwalten, setzen Sie bitte die Regeln im Virtual LAN (VLAN) Menü.



5.2.2 Basiskonfiguration

Diese Seite beinhaltet die allgemeinen LAN-Einstellungen.

Klicken Sie auf **LAN**, um die Seite mit den LAN-Einstellungen zu öffnen, und wählen Sie **Basiskonfiguration**.



NAT IP-Adresse - Geben Sie die private IP-Adresse für die Verbindung zu einem lokalen privaten Netzwerk ein (Standard: 192.168.1.1).

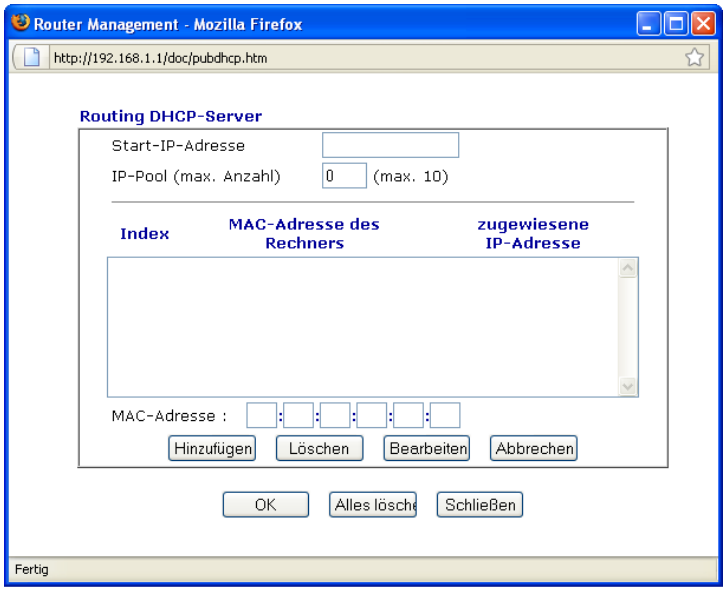
Subnetz-Maske - Geben Sie den Adressbereich ein, der die Größe des Netzwerks bestimmt. (Standard: 255.255.255.0/ 24)

IP-Routing - Klicken Sie auf **Aktiv**, um diese Funktion zu starten. Die Standardeinstellung ist **Inaktiv**.

Routing IP-Adresse - Geben Sie die 2. IP-Adresse für die Verbindung zu einem Subnetz ein. (Standard: 192.168.2.1/ 24)

Subnetz-Maske - Ein Adressbereich, der die Größe des Netzwerks bestimmt. (Standard: 255.255.255.0/ 24)

Routing DHCP-Server - Sie können den Router als DHCP-Server für das zweite Subnetz einrichten.



Start-IP-Adresse: - Geben Sie einen Wert aus dem IP-Adresspool an, bei dem der DHCP-Server bei der Vergabe von IP-Adressen anfangen soll. Falls die Routing-IP-Adresse Ihres Routers 220.135.240.1 ist, muss die Start-IP-Adresse 220.135.240.2 oder größer, jedoch kleiner als 220.135.240.254 sein.

IP-Pool (Anzahl): - Geben Sie die Anzahl der IP-Adressen in diesem Pool an. Die maximale Anzahl beträgt 10. Wenn Sie zum Beispiel 3 eingeben und die Routing-IP-Adresse Ihres Routers 220.135.240.1 ist, so reicht der IP-Adressbereich des DHCP-Servers von 220.135.240.2 bis 220.135.240.4.

MAC-Adresse: - Geben Sie die MAC-Adressen der Hosts nacheinander ein und klicken Sie auf **Hinzufügen**, um eine Liste der Hosts zu erstellen, denen aus dem oben erwähnten Pool IP-Adressen zugewiesen, gelöscht oder geändert werden sollen. Die Erstellung einer Liste von MAC-Adressen für den Routing-DHCP-Server ermöglicht dem Router, den richtigen Hosts die richtigen IP-Adressen des richtigen Subnetzes zuzuweisen. So wird vermieden, dass den Hosts im Routing-Subnetz IP-Adressen aus dem NAT-Subnetz zugewiesen werden.

RIPInaktiv - deaktiviert das RIP-Protokoll. Damit wird zwischen Routern keine Routing-Information ausgetauscht. (Standardeinstellung)

NAT-Subnetz - Lässt den Router die RIP-Information des NAT-Subnetzes mit benachbarten Routern austauschen.

Routing-Subnetz - Lässt den Router die RIP-Information des Routing-Subnetzes mit benachbarten Routern austauschen.

DHCP-Serverkonfiguration - DHCP ist die Abkürzung für Dynamic Host Configuration Protocol. Der Router dient standardmäßig als DHCP-Server für Ihr Netzwerk und sendet automatisch IP-bezogene Einstellungen an alle lokalen Rechner, die als DHCP-Clients konfiguriert sind. Es wird empfohlen, den Router als DHCP-Server aktiviert zu lassen, sofern Sie für Ihr Netzwerk keinen gesonderten DHCP-Server haben.

Falls Sie im Netzwerk nicht den Vigor-Router, sondern einen anderen Rechner als DHCP-Server benutzen möchten, können Sie den Relay-Agent verwenden, um die DHCP-Anforderungen an den jeweiligen Rechner umzuleiten.

Aktiv - Lässt den Router jedem Host im LAN IP-Adressen zuweisen.

Inaktiv – Lässt Sie manuell jedem Host im LAN IP-Adressen zuweisen.

Relay-Agent – (NAT-Subnetz/Routing-Subnetz) Geben Sie das Subnetz an, in dem sich der DHCP-Server befindet, an den der Relay-Agent die DHCP-Anforderungen weiterleiten soll.

Start-IP-Adresse - Geben Sie einen Wert aus dem IP-Adresspool an, bei dem der DHCP-Server bei der Vergabe von IP-Adressen anfangen soll. Falls die erste IP-Adresse Ihres Routers 192.168.1.1 ist, muss die Start-IP-Adresse 192.168.1.2 oder größer, jedoch kleiner als 192.168.1.254 sein.

IP-Pool (Anzahl) - Geben Sie die maximale Anzahl der Rechner an, denen der DHCP-Server IP-Adressen zuweisen soll. Der Standardwert beträgt 50, und die maximale Anzahl ist 253.

Gateway-IP-Adresse - Geben Sie die Gateway-IP-Adresse für den DHCP-Server ein. Der Wert entspricht üblicherweise der ersten IP-Adresse des Routers, d.h. der Router ist das Standard-Gateway.

DHCP-Server-IP für Relay-Agent - Setzen Sie die IP-Adresse des DHCP-Servers, den Sie verwenden möchten, damit der Relay-Agent die DHCP-Anforderungen an diesen DHCP-Server weiterleiten kann.

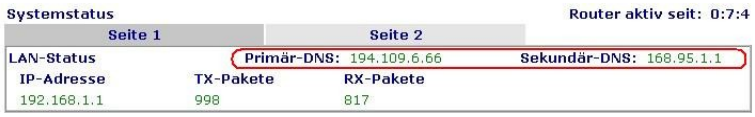
DNS-Serverkonfiguration - DNS ist die Abkürzung für Domain Name System. Jeder Internet-Host muss eine eindeutige IP-Adresse haben und kann auch einen Namen tragen, der einfach zu merken ist, wie z.B. www.yahoo.com. Der DNS-Server wandelt den benutzerfreundlichen Namen in die entsprechende IP-Adresse um.

Folgende DNS-Einstellungen verwenden - Den Vigor-Router zwingen, nicht die vom Internetzugangsserver bestimmten DNS-Server (PPPoE, PPTP, L2TP oder DHCP-Server), sondern die DNS-Server auf dieser Seite zu verwenden.

Primäre IP-Adresse - Geben Sie hier die IP-Adresse eines DNS-Servers ein, dessen Daten Ihnen Ihr ISP mitgeteilt haben sollte. Falls der ISP diese Daten nicht bereitstellt, trägt der Router automatisch die IP-Adresse des Standard-DNS-Servers in diesem Feld ein: 194.109.6.66.

Sekundäre IP-Adresse - Hier können Sie eine alternative DNS-Server-IP eintragen, falls der ISP Ihnen die Daten mehrerer DNS-Server mitgeteilt hat. Falls der ISP diese Daten nicht bereitstellt, trägt der Router automatisch die IP-Adresse des standardmäßigen alternativen DNS-Servers in diesem Feld ein: 194.98.0.1.

Die Standard-DNS-Server-IP ist unter dem Onlinestatus sichtbar:



Falls die Felder für die IP-Adressen des bevorzugten DNS-Servers und des alternativen DNS-Servers nicht ausgefüllt werden, weist der Router seine eigene IP-Adresse als DNS-Proxy-Server für lokale Benutzer zu und unterhält einen DNS-Cache.

Falls die IP-Adresse eines Domain-Namens bereits im DNS-Cache vorhanden ist, löst der Router den Domain-Namen sofort auf. Andernfalls leitet der Router die DNS-Anfrage über die WAN-Verbindung (z.B. DSL, Kabel) an den externen DNS-Server weiter.

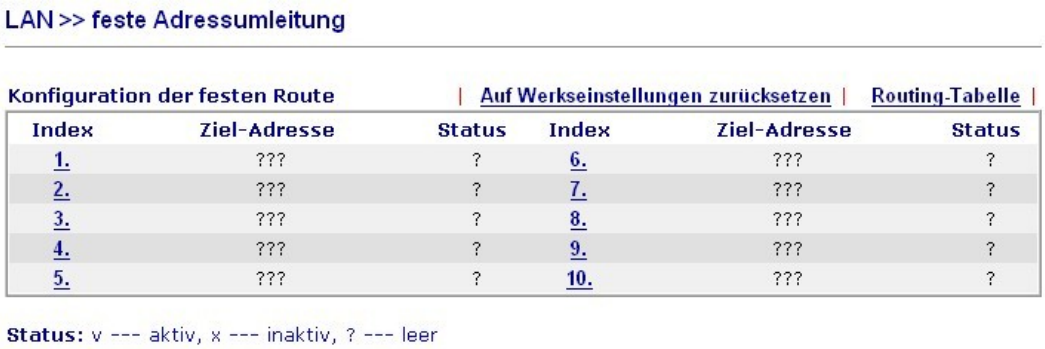
In Kapitel 4 werden zwei übliche Szenarien für LAN-Einstellungen vorgestellt. Neben Einzelheiten zu den Konfigurationsbeispielen enthält das Kapitel weitere Informationen für Ihre Bedürfnisse.

5.2.3 Feste Adressumleitung

Gehen Sie zur Seite mit den Einstellungen für das **LAN** und wählen Sie **Feste Adressumleitung**.

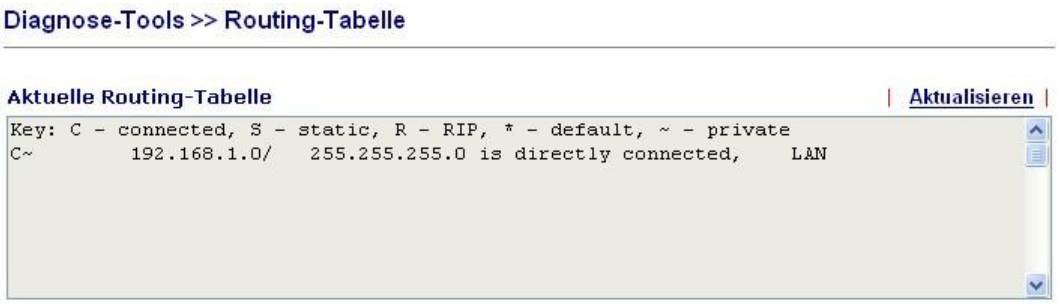
Index - Die Nummern 1 bis 10 unter Index ermöglichen Ihnen, auf die nächste Seite zu gelangen, um die feste Adressumleitung einzurichten.

Zieladresse - Zeigt die Zieladresse der festen Adressumleitung an.


LAN >> feste Adressumleitung
Konfiguration der festen Route | Auf Werkseinstellungen zurücksetzen | Routing-Tabelle |
Index Ziel-Adresse Status Index Ziel-Adresse Status
1. ??? ? 6. ??? ?
2. ??? ? 7. ??? ?
3. ??? ? 8. ??? ?
4. ??? ? 9. ??? ?
5. ??? ? 10. ??? ?
Status: v --- aktiv, x --- inaktiv, ? --- leer

Status - Zeigt den Status der festen Adressumleitung an.

Routing-Tabelle anzeigen - Zeigt die Routing-Tabelle an.


Diagnose-Tools >> Routing-Tabelle
Aktuelle Routing-Tabelle | Aktualisieren |
Key: C - connected, S - static, R - RIP, * - default, ~ - private
C~ 192.168.1.0/ 255.255.255.0 is directly connected, LAN

Hinzufügen von festen Adressumleitungen zu privaten und öffentlichen Netzwerken

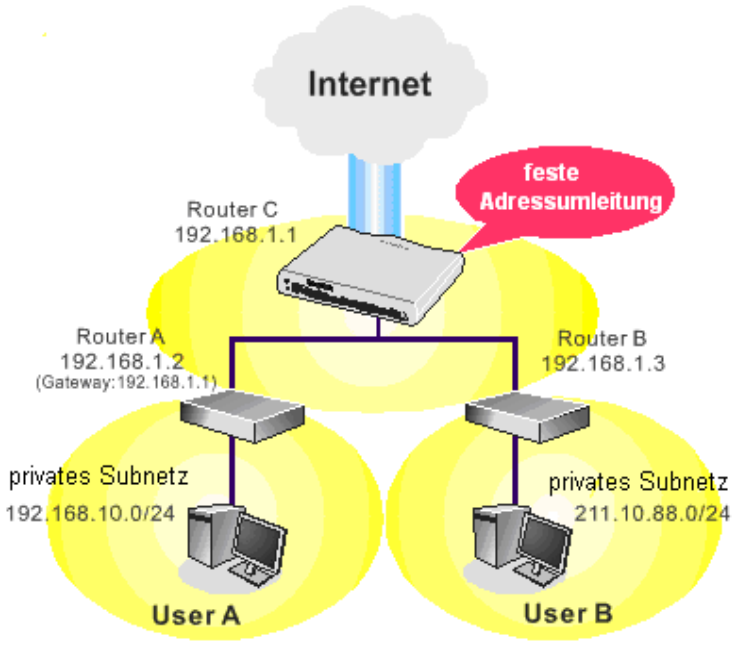
Es folgt ein Konfigurationsbeispiel für eine feste Adressumleitung im Hauptrouter, so dass die Benutzer A und B, die sich in unterschiedlichen Subnetzen befinden, über den Router miteinander kommunizieren können. Es wird angenommen, dass der Internetzugang bereits eingerichtet worden ist und der Router ordnungsgemäß funktioniert.

- Der Hauptrouter wird zum Surfen im Internet verwendet.
- Einrichtung eines privaten Subnetzes 192.168.10.0 mit dem internen Router A (192.168.1.2)
- Einrichtung eines öffentlichen Subnetzes 211.100.88.0 über den internen Router B (192.168.1.3).
- Konfiguration des Hauptrouters 192.168.1.1 als Standard-Gateway für den Router A (192.168.1.2).

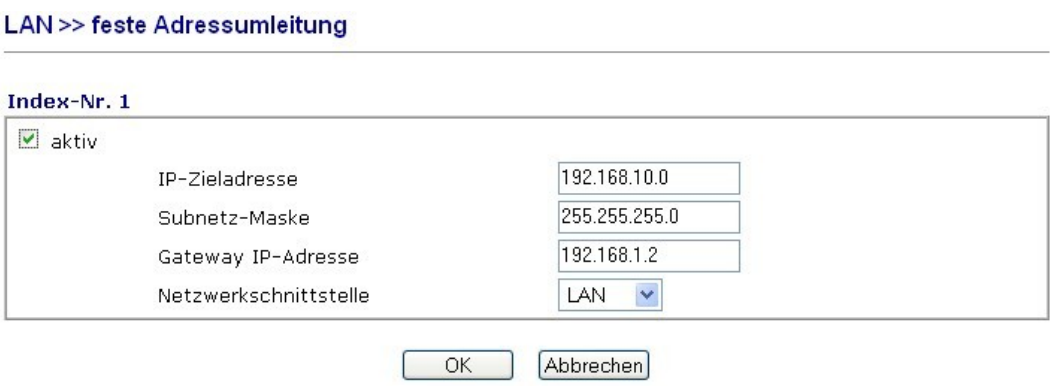
Vor Einrichtung der festen Adressumleitung kann Benutzer A nicht mit Benutzer B kommunizieren, da Router A nur anerkannte Pakete an den Hauptrouter als Standard-Gateway leiten kann.

1. Gehen Sie zur **LAN**-Seite, klicken auf **Basiskonfiguration** und wählen das erste Subnetz als **RIP**. Klicken Sie dann auf **OK**.

Hinweis: Es gibt zwei Gründe für die Anwendung von RIP im ersten Subnetz. Der erste ist, dass die LAN-Schnittstelle über das erste Subnetz (192.168.1.0/24) RIP-Pakete mit benachbarten Routern austauschen kann. Der zweite Grund besteht darin, dass diese Hosts in internen privaten Subnetzen (z.B. 192.168.10.0/24) über den Router auf das Internet zugreifen können und ständig IP-Routing-Informationen mit anderen Subnetzen austauschen können.

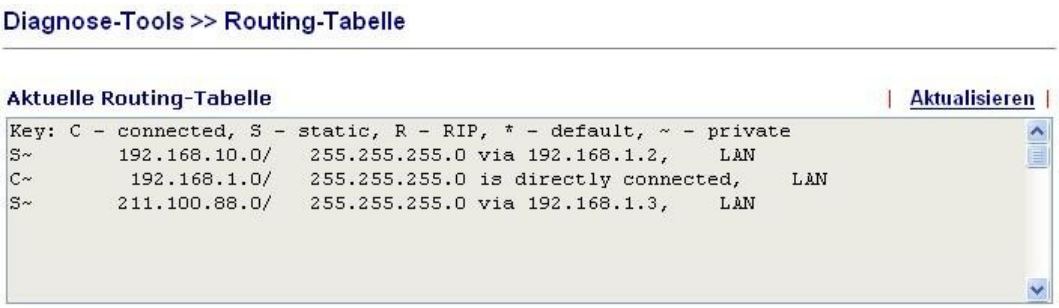


2. Wählen Sie **LAN - Feste Adressumleitung** und klicken Sie auf die **Indexnummer 1.** Fügen Sie wie unten gezeigt eine feste Adressumleitung hinzu, die festlegt, dass alle für 192.168.10.0 bestimmten Pakete an 192.168.1.2 umgeleitet werden. Klicken Sie auf **OK**.



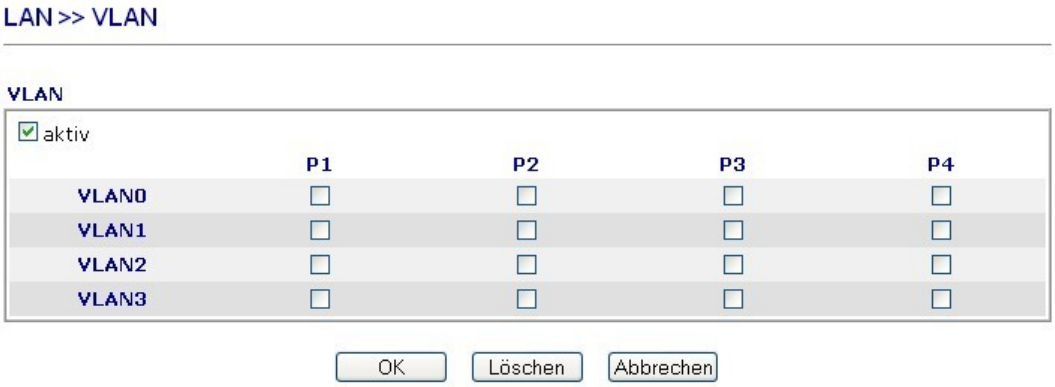
3. Kehren Sie zurück zur Seite **Feste Adressumleitung**. Klicken Sie auf eine andere **Indexnummer**, um wie unten gezeigt eine weitere feste Adressumleitung hinzuzufügen, die festlegt, dass alle für 211.100.88.0 bestimmten Pakete an 192.168.1.3 umgeleitet werden.

4. Gehen Sie zu **Diagnose-Tools** und wählen Sie **Routing-Tabelle**, um die aktuelle Routing-Tabelle zu verifizieren.


Diagnose-Tools >> Routing-Tabelle
Aktuelle Routing-Tabelle
Aktualisieren
Key: C - connected, S - static, R - RIP, * - default, ~ - private
S~ 192.168.10.0/ 255.255.255.0 via 192.168.1.2, LAN
C~ 192.168.1.0/ 255.255.255.0 is directly connected, LAN
S~ 211.100.88.0/ 255.255.255.0 via 192.168.1.3, LAN

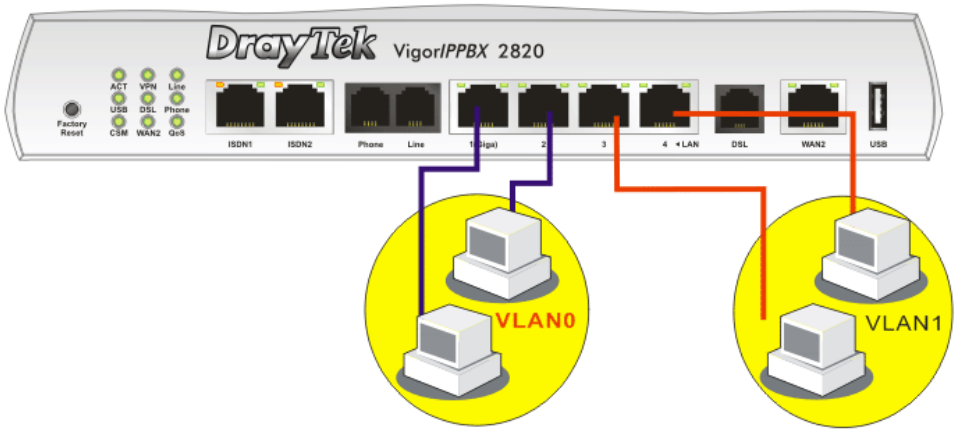
5.2.4 VLAN

Die Virtual LAN Funktion bietet eine komfortable Möglichkeit, Hosts zu verwalten, indem diese auf der Grundlage des physischen Ports gruppiert werden. Sie können außerdem die Ein- und Ausgangsgeschwindigkeit jedes Ports einstellen. Gehen Sie zur **LAN**-Seite und wählen Sie **VLAN**. Die folgende Seite erscheint. Klicken Sie auf **Aktiv**, um die VLAN-Funktion zu starten.



Das folgende Beispiel zeigt, wie man ein VLAN hinzufügen oder entfernen kann.

1. Falls VLAN 0 aus Hosts besteht, die mit P1 und P2 verbunden sind, so besteht VLAN 1 aus Hosts, die mit P3 und P4 verbunden sind.



2. Haken Sie das Kästchen zur Aktivierung der VLAN-Funktion an und markieren Sie die unten gezeigte Tabelle gemäß Ihren Anforderungen.

LAN >> VLAN

VLAN

aktiv

	P1	P2	P3	P4
VLAN0	☑	☑	☐	☐
VLAN1	☐	☐	☑	☑
VLAN2	☐	☐	☐	☐
VLAN3	☐	☐	☐	☐

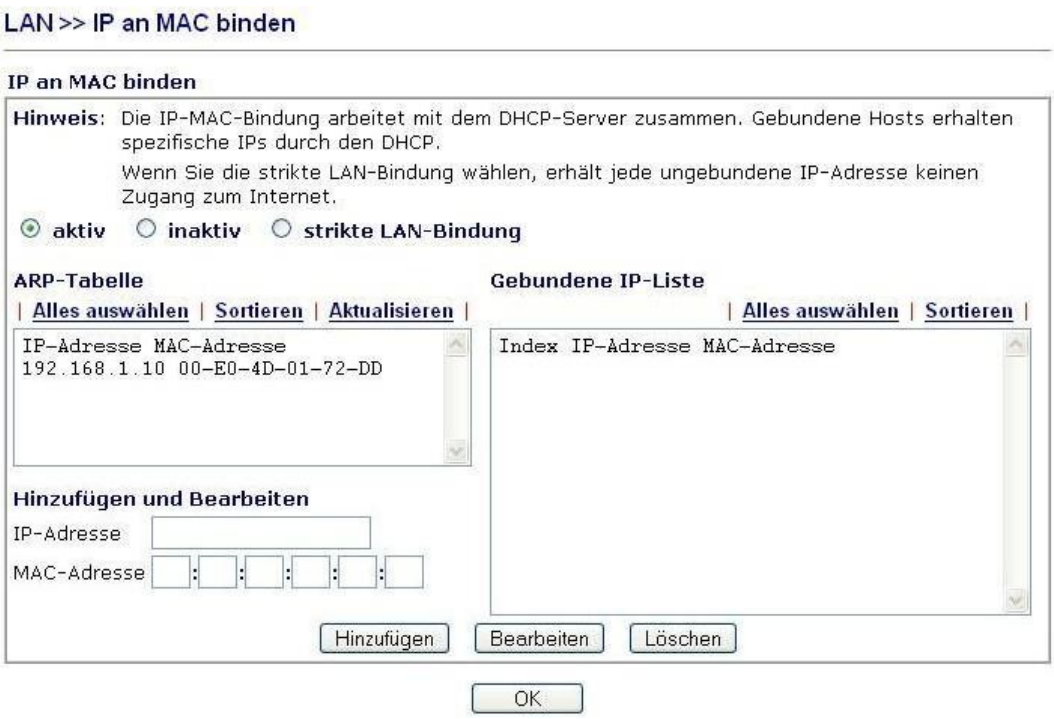
OK Löschen Abbrechen

Um VLAN zu entfernen, deaktivieren Sie das entsprechende Kästchen und klicken auf **OK**, um das Ergebnis zu speichern.

5.2.5 IP an MAC binden

Diese Funktion wird verwendet, um zwecks besserer Kontrolle im LAN die IP-Adresse an die MAC-Adresse zu binden. Falls diese Funktion aktiviert ist, können die zugewiesenen IP-/MAC-Bindungen nicht geändert werden. Änderungen der gebundenen IP- bzw. MAC-Adresse können dazu führen, dass Ihr Zugriff auf das Internet blockiert wird.

Klicken Sie auf **LAN** und wählen Sie **IP an MAC binden**, um die Seite mit den Einstellungen zu öffnen.



Aktiv - Klicken Sie auf diese Taste, um diese Funktion zu aktivieren. Es können jedoch auch IP-/MAC-Paare, die nicht in der Liste aufgeführt sind, auf das Internet zugreifen.

Inaktiv - Klicken Sie auf diese Taste, um diese Funktion zu deaktivieren. Alle Einstellungen auf dieser Seite werden ungültig.

Strikte LAN-Bindung - Klicken Sie auf diese Taste, um IP-/MAC-Bindungen zu blockieren, die nicht in der Liste aufgeführt sind.

ARP-Tabelle - Dies ist die LAN ARP-Tabelle dieses Routers. Die IP- und MAC-Information erscheint in diesem Feld. Jedes in der ARP-Tabelle aufgeführte IP-/MAC-Paar kann ausgewählt und durch Klicken auf **Hinzufügen** der gebundenen IP-Liste hinzugefügt werden.

Hinzufügen und bearbeitenIP-Adresse – Geben Sie die IP-Adresse ein, die für die angegebene MAC-Adresse zu verwenden ist.

MAC-Adresse – Geben Sie die MAC-Adresse ein, die an die entsprechende IP-Adresse

gebunden werden soll.

Aktualisieren - Klicken Sie hier, um die ARP-Tabelle zu aktualisieren. Wenn dem LAN ein neuer Rechner hinzugefügt wird, können Sie hier klicken, um die aktuellen Informationen in der ARP-Tabelle zu sehen.

Gebundene IP-Liste - Zeigt eine Liste der IP-Adressen an, die an MAC-Adressen gebunden sind.

Hinzufügen - Mit dieser Aktion können Sie das aus der ARP-Tabelle gewählte oder unter **Hinzufügen und bearbeiten** eingegebene IP/MAC-Paar der Tabelle **Gebundene IP-Liste** hinzufügen.

Bearbeiten - Ermöglicht Ihnen, die gewählte IP-Adresse und die MAC-Adresse zu bearbeiten und zu ändern, die Sie zuvor erstellt hatten.

Entfernen - Sie können jeden Eintrag aus der **Gebundenen IP-Liste** entfernen. Zur Auswahl klicken Sie einfach einen Eintrag an und klicken auf **Entfernen**. Der gewählte Eintrag wird aus der **Gebundenen IP-Liste** entfernt.

Hinweis: Bevor Sie **Strikte LAN-Bindung** wählen, müssen Sie einen IP-/MAC-Adresssatz für einen PC binden. Falls dies nicht geschieht, kann keiner der Rechner auf das Internet zugreifen. Außerdem ist es möglicherweise nicht mehr möglich, auf das Router-Menü zuzugreifen.

5.3 NAT

Normalerweise dient der Router als NAT-Router (Network Address Translation). Der NAT-Mechanismus ermöglicht die Verwendung von einer oder mehreren privaten IP-Adressen mit einer öffentlichen IP-Adresse. Die öffentliche IP-Adresse wird gewöhnlich von Ihrem ISP zugewiesen. Private IP-Adressen werden nur zwischen internen Hosts erkannt.

Wenn abgehende Pakete, die an einen öffentlichen Server im Internet gerichtet sind, beim NAT-Router ankommen, ändert der Router deren Quelladresse in die öffentliche IP-Adresse des Routers, wählt den verfügbaren Port und leitet die Pakete weiter. Gleichzeitig macht der Router in einer Tabelle einen Eintrag, um sich diese Adress-/Portzuordnung zu merken. Wenn der öffentliche Server antwortet, ist der eingehende Verkehr natürlich an die öffentliche IP-Adresse des Routers gerichtet, weshalb der Router anhand der Tabelle die Umwandlung vornimmt. So ist es einem internen Host möglich, flüssig mit einem externen Host zu kommunizieren.

Einige Vorteile von NAT:

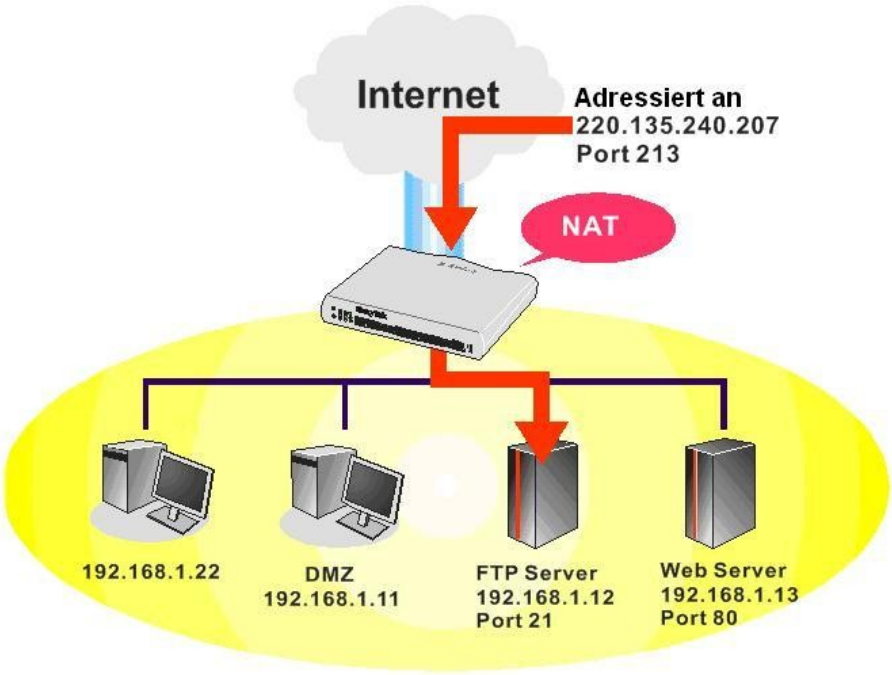
- **Einsparung von Kosten für öffentliche IP-Adressen und effizienter Einsatz der IP-Adresse.** NAT ermöglicht die Übersetzung der internen IP-Adressen lokaler Hosts in eine einzige öffentliche IP-Adresse, so dass für sämtliche interne Hosts lediglich eine IP-Adresse erforderlich ist.
- **Höhere Sicherheit des internen Netzwerks durch Verdeckung der internen IP-Adresse.** Es gibt viele Arten von Angriffen auf Grundlage der IP-Adresse. Da der Angreifer die internen IP-Adressen nicht kennt, stellt die NAT-Funktion einen Schutz für das interne Netzwerk dar.

Auf der NAT-Seite sehen Sie die in RFC-1918 definierte private IP-Adresse. Normalerweise wird das Subnetz 192.168.1.0/24 für den Router verwendet. Wie oben erwähnt, kann die NAT-Funktion verschiedenen Diensten eine oder mehrere IP-Adressen oder Ports zuordnen, d.h. die NAT-Funktion verwendet Port-Zuordnungsmethoden.

Die folgende Abbildung zeigt die Menüeinträge für NAT:

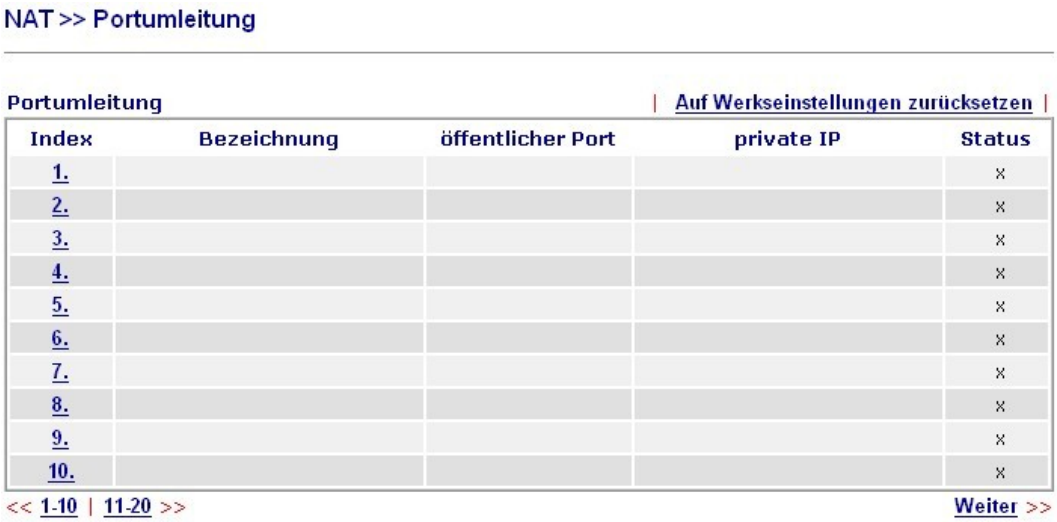
5.3.1 Portumleitung

Portumleitung wird gewöhnlich für serverbezogene Dienste im lokalen Netzwerk genutzt, z.B. für Web-Server, FTP-Server, E-Mail-Server, usw. Meistens benötigen Sie für jeden Server eine öffentliche IP-Adresse, und diese öffentliche IP-Adresse/Domain-Name wird von allen Benutzern erkannt. Da der Server sich jedoch innerhalb des LANs befindet, das Netzwerk vom NAT des Routers geschützt wird und unter seiner privaten IP-Adresse/Port identifiziert wird, besteht der Zweck der Portumleitung darin, alle Zugriffe mit öffentlicher IP-Adresse von externen Benutzern an die private IP-Adresse/Port des Servers umzuleiten.

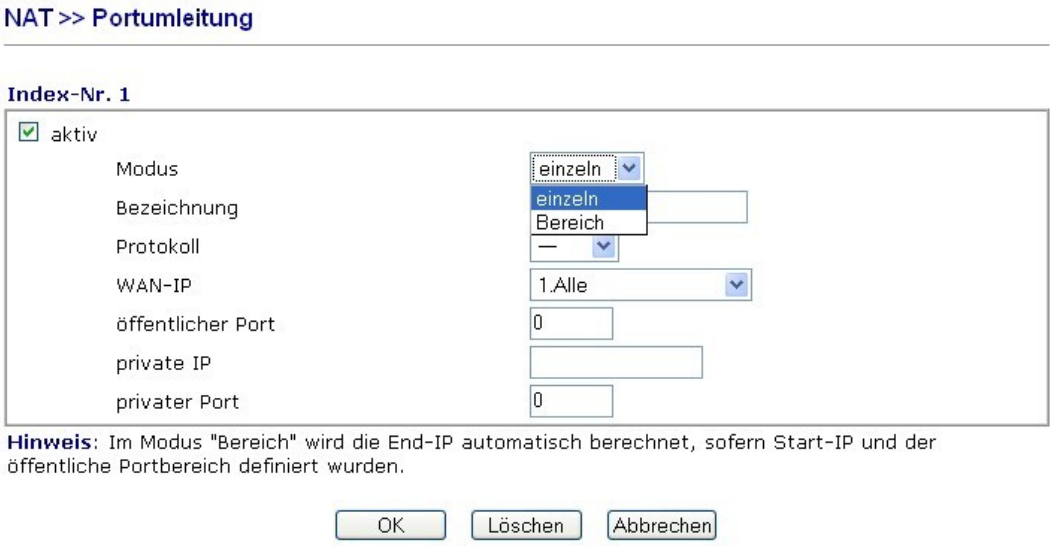


Die Portumleitung ist nur für eingehenden Datenverkehr möglich.

Um diese Funktion zu nutzen, gehen Sie zur **NAT**-Seite und wählen **Portumleitung**. Die **Portumleitungstabelle** ermöglicht 20 Port-Zuordnungseinträge für die internen Hosts.



Klicken Sie auf eine beliebige Nummer unter "Index" um auf die nächste Seite für die Konfiguration der Portumleitung zu gelangen.



Aktiv - Markieren Sie dieses Kästchen, um die Portumleitung zu aktivieren.

Modus - Es stehen hier zwei Optionen (Einzeln und Bereich) zur Auswahl. Um für den Dienst einen Bereich zu bestimmen, wählen Sie **Bereich**. Bei Eingabe der öffentlichen Ports (Startport und Endport) und der Start-IP des privaten IP-Adressbereichs im Bereichsmodus berechnet das System automatisch die End-IP des privaten IP-Adressbereichs und zeigt diese an.

Bezeichnung - Geben Sie eine Beschreibung des jeweiligen Netzwerkdienstes ein.

Protokoll - Wählen Sie das Protokoll für die

Transportschicht (TCP oder UDP).

WAN-IP - Bestimmen Sie die WAN-IP für die Portumleitung. Es stehen acht IP-Aliasse zur Auswahl, die für die Portumleitung verwendet werden können. Die Standardeinstellung ist **Alle**, was bedeutet, dass sämtliche eingehende Daten von jedem Port zum angegebenen IP-Adress- und Portbereich weitergeleitet werden.

Öffentlicher Port - Geben Sie an, welcher Port an die angegebene **private IP und Port** des internen Hosts umgeleitet werden soll. Falls Sie **Bereich** als Portumleitungsmodus wählen, sehen Sie in diesem Feld zwei Kästchen. Geben Sie die gewünschte Nummer im ersten Kästchen ein. Das zweite Kästchen wird danach automatisch ausgefüllt.

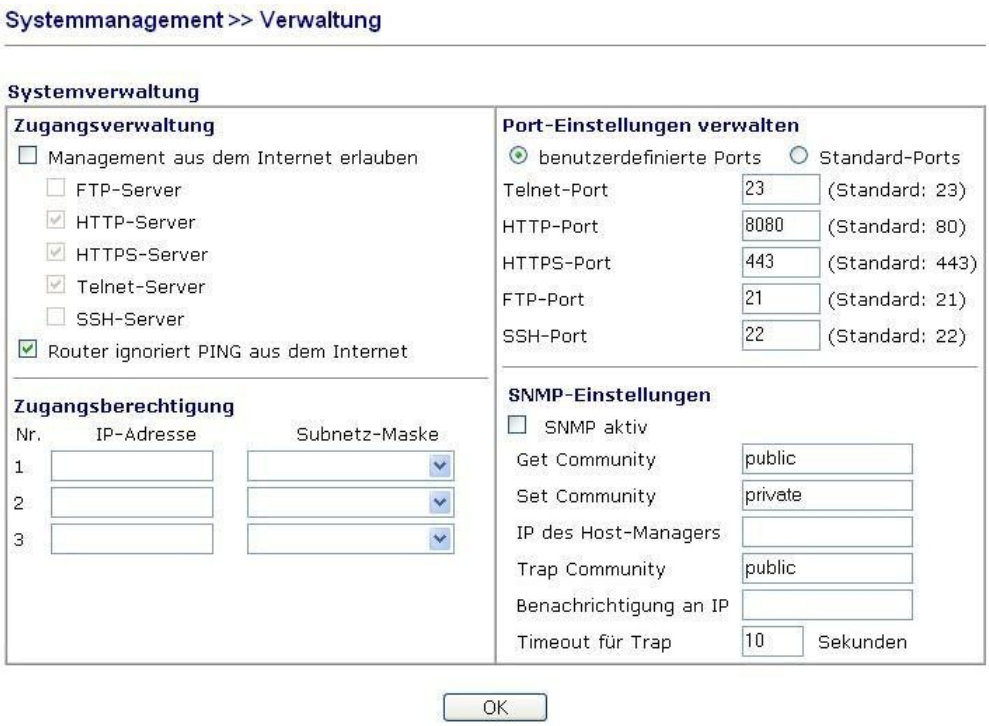
Private IP - Geben Sie die private IP-Adresse des internen Hosts an, der den Dienst anbietet. Falls Sie **Bereich** als Portumleitungsmodus wählen, sehen Sie in diesem Feld zwei Kästchen. Geben Sie im ersten Kästchen eine komplette IP-Adresse ein (als Anfangspunkt) und die vierte Zifferngruppe im zweiten Kästchen (als Endpunkt).

Privater Port - Geben Sie die private Portnummer des Dienstes an, den der interne Host anbietet.

Aktiv - Markieren Sie dieses Kästchen, um die definierte Port-Zuordnung zu aktivieren.

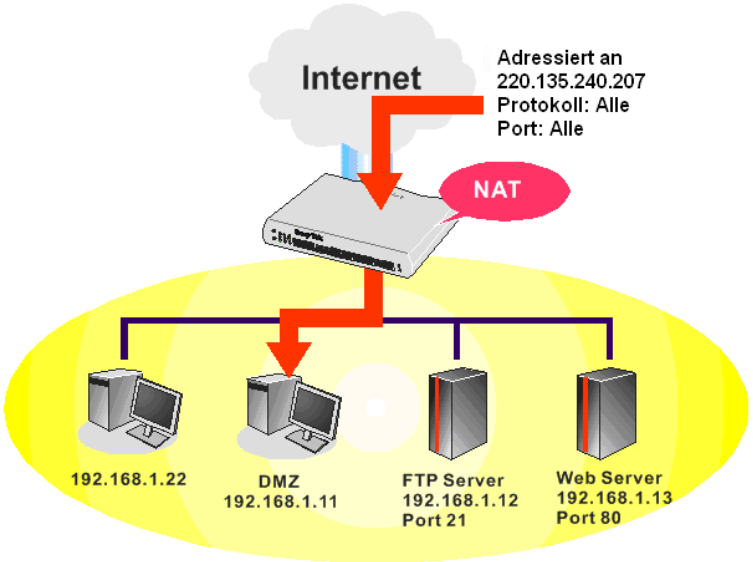
Der Router verfügt über eingebaute Dienste (Server) wie Telnet, HTTP, FTP, usw. Da diese Dienste (Server) immer die gleichen Portnummern verwenden, kann es notwendig sein, die Portnummern des Routers zu ändern, um Konflikte zu vermeiden.

Das Router-Menü beispielsweise verwendet den Standardport 80, was einen Konflikt mit dem Webserver im lokalen Netzwerk (http://192.168.1.13:80) verursachen kann. **Ändern Sie daher den HTTP-Port des Routers auf einen anderen Port als den Standardport 80**, um einen Konflikt zu vermeiden, z.B. auf 8080. Dies kann unter **Systemmanagement >>Systemverwaltung** eingestellt werden. Danach haben Sie über Port 8080 Zugriff auf das Administrationsmenü (z.B. http://192.168.1.1:8080), nicht mehr über Port 80.



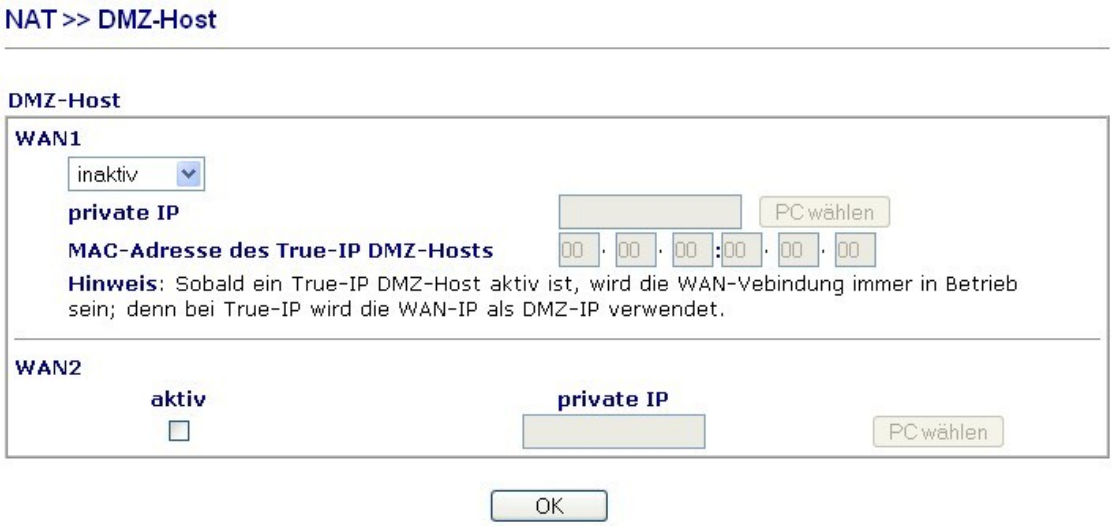
5.3.2 DMZ-Host

Wie oben erwähnt, kann die **Portumleitung** eingehenden TCP-/UDP-Verkehr oder anderen Verkehr auf bestimmten Ports an die angegebene private IP-Adresse/Port des Hosts im LAN umleiten. Es ist jedoch zu beachten, dass andere IP-Protokolle wie z.B. die Protokolle 50 (ESP) und 51 (AH) nicht auf einem festen Port kommunizieren. Der Vigor-Router bietet eine **DMZ-Host**-Funktion, die sämtliche unangeforderte Daten auf beliebigen Protokollen einem einzigen Host im LAN zuordnet. Normales Web-Surfen und andere Internet-Aktivitäten anderer Clients funktionieren weiterhin ohne unangemessene Unterbrechung. **DMZ-Host** ermöglicht einem definierten internen Benutzer, dem Internet vollständig ausgesetzt zu sein, was für gewisse Anwendungen wie Netmeeting oder Internet-Spiele usw. notwendig sein mag.

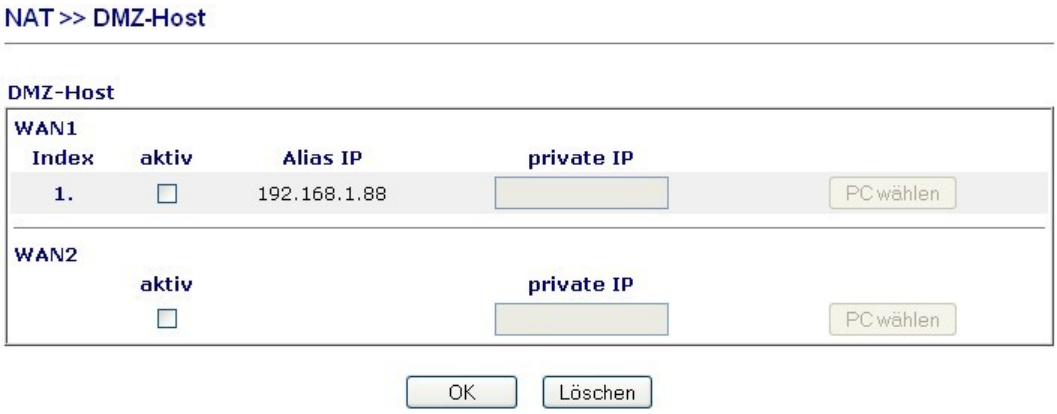


Die Sicherheitseigenschaften von NAT werden umgangen, wenn Sie einen DMZ-Host einrichten. Wir empfehlen Ihnen daher, zusätzliche Filterregeln oder eine zweite Firewall zu konfigurieren.

Klicken Sie auf **DMZ-Host**, um die folgende Seite zu öffnen:



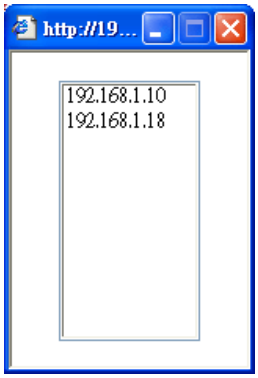
Falls Sie zuvor einen **WAN-Alias** für den **PPPoE/PPPoA** oder **MPoA**-Modus eingerichtet haben, finden Sie diesen unter **Alias IP** zur Auswahl.



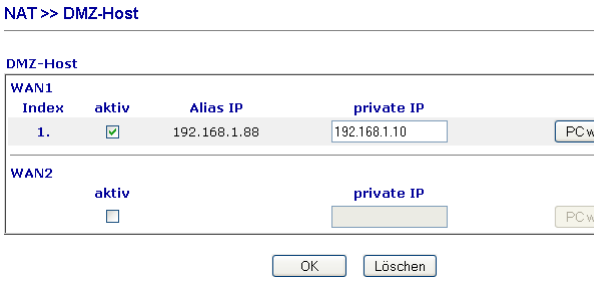
Aktiv - Markieren Sie dieses Kästchen, um die DMZ-Host-Funktion zu aktivieren.

Private IP - Geben Sie die private IP-Adresse des DMZ-Hosts ein oder klicken Sie auf "PC wählen", um eine IP-Adresse zu wählen.

PC wählen - Wenn Sie auf diese Taste klicken, öffnet sich automatisch das unten abgebildete Fenster. Das Fenster enthält eine Liste privater IP-Adressen aller Hosts in Ihrem LAN. Bestimmen Sie eine private IP-Adresse aus der Liste als DMZ-Host.



Nachdem Sie im gezeigten Dialog eine private IP gewählt haben, wird die IP-Adresse im folgenden Fenster angezeigt. Klicken Sie auf **OK**, um diese Einstellung zu speichern.



5.3.3 Offene Ports

Offene Ports ermöglicht Ihnen, einen Portbereich für den Verkehr besonderer Anwendungen zu öffnen. Bestimmte Ports müssen beispielsweise für P2P-Anwendungen (BT, KaZaA, Gnutella, WinMX, eMule usw.), Webcam usw. geöffnet werden. Sorgen Sie dafür, dass die betreffende Anwendung immer auf dem neuesten Stand ist, um Angriffe auf eventuelle Sicherheitslücken zu vermeiden.

Klicken Sie auf **Offene Ports**, um die folgende Seite zu öffnen:

Index - Geben Sie die relative Nummer eines bestimmten Eintrags an, für den Sie einen Dienst auf einem lokalen Host anbieten möchten. Klicken Sie auf die entsprechende Indexnummer, um den Eintrag zu bearbeiten oder zu löschen.

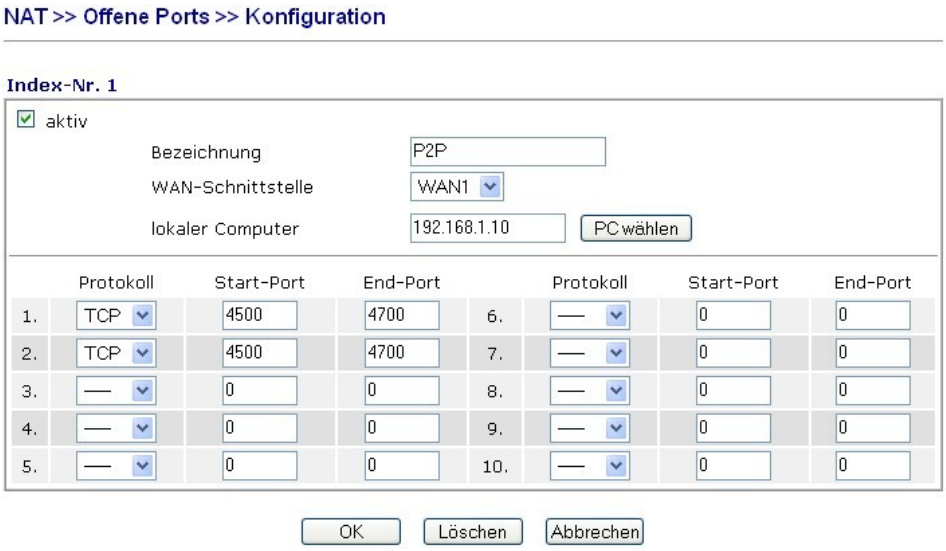
Bezeichnung - Geben Sie die Bezeichnung des definierten Netzwerkdienstes an.

WAN-Schnittstelle - WAN-Schnittstelle für den Eintrag anzeigen.

Lokale IP-Adresse - Private IP-Adresse des lokalen Hosts anzeigen, der den Dienst anbietet.

Status - Status des entsprechenden Eintrags anzeigen. X oder V steht für **Inaktiv** bzw. **Aktiv**.

Um Porteinstellungen hinzuzufügen oder zu bearbeiten, klicken Sie auf eine der Indexnummern auf der Seite. Die Konfigurationsseite für den Indexeintrag erscheint. In jedem Indexeintrag können Sie **10** Portbereiche für verschiedene Dienste angeben.



Aktiv - Markieren Sie dieses Kästchen, um diesen Eintrag zu aktivieren.

Bezeichnung - Geben Sie die Bezeichnung der definierten Netzwerkanwendung/des definierten Netzwerkdienstes an.

WAN-Schnittstelle - Geben Sie die WAN-Schnittstelle an, die für diesen Eintrag verwendet werden soll.

Lokaler Computer - Geben Sie die private IP-Adresse des lokalen Hosts ein oder klicken Sie auf **PC wählen**, um eine IP-Adresse zu wählen.

PC wählen - Wenn Sie auf diese Taste klicken, öffnet sich automatisch ein Fenster mit einer Liste privater IP-Adressen von lokalen Hosts. Wählen Sie die entsprechende IP-Adresse des lokalen Hosts aus der Liste.

Protokoll -Wählen Sie das Protokoll für die Transportschicht. Zur Auswahl stehen **TCP**, **UDP** oder **-----** (keines).

Start-Port - Geben Sie die Start-Portnummer des Dienstes an, den der interne Host anbietet.

End-Port - Geben Sie die End-Portnummer des Dienstes an, den der interne Host anbietet.

5.4 Firewall

5.4.1 Firewall-Grundlagen

Der zunehmende Bedarf nach Bandbreite für Multimedia, interaktive Anwendungen und Fernunterricht steht verschiedenen Sicherheitsbedenken gegenüber. Die Firewall des Vigor-Routers ermöglicht Ihnen, Ihr lokales Netzwerk vor Angriffen Unbefugter zu schützen. Die Firewall kann auch die Nutzung des Internet durch Benutzer im lokalen Netzwerk beschränken. Außerdem ist es möglich, gewisse Pakete zu verwerfen, die den Router veranlassen würden, eine unerwünschte Verbindung nach außen aufzubauen.

Eigenschaften der Firewall

Die folgenden Firewall-Eigenschaften schützen die Benutzer im LAN:

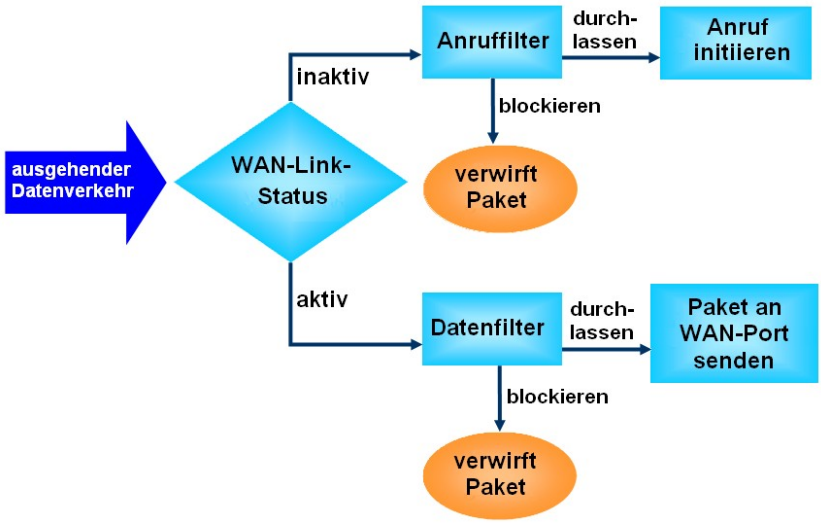
- Benutzerabhängige IP-Filter (Anruffilter/Datenfilter)
- SPI (Stateful Packet Inspection) kontrolliert Pakete und blockiert nicht angeforderte eingehende Daten.
- Optionaler Schutz vor DoS/DDoS-Angriffen

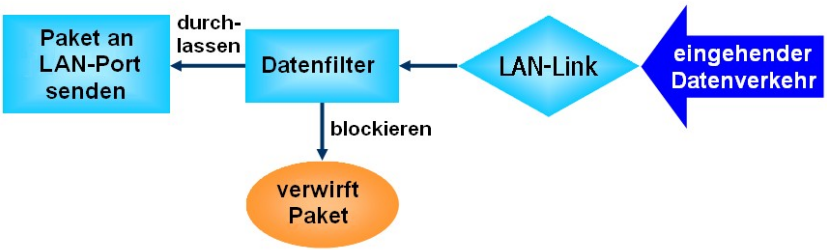
IP-Filter

Je nachdem, ob eine Internet-Verbindung existiert oder nicht, d.h. je nachdem, ob die WAN-Verbindung aktiv ist oder nicht, unterscheidet die IP-Filterarchitektur zwei Arten von Filtern: **Anruffilter** und **Datenfilter**.

- **Anruffilter -** Falls keine Verbindung zum Internet besteht, wird der **Anruffilter** auf den ausgehenden Verkehr angewendet. Er überprüft die Pakete gemäß den Filterregeln. Zulässige Pakete werden durchgelassen. Der Router veranlasst daraufhin einen **Anruf**, um die Internet-Verbindung aufzubauen und das Paket über das Internet zu versenden.
- **Datenfilter** - Falls eine Verbindung zum Internet besteht, wird der **Datenfilter** auf den ein- und ausgehenden Verkehr angewendet. Er überprüft die Pakete gemäß den Filterregeln. Zulässige Pakete werden durch den Router durchgelassen.

Die folgenden Flussdiagramme veranschaulichen, wie der Router mit ein- und ausgehendem Verkehr umgeht.





Stateful Packet Inspection (SPI)

Stateful Inspection ist eine Firewall-Architektur, die auf der Netzwerkschicht implementiert ist. Im Gegensatz zur herkömmlichen statischen Paketfilterung, welche ein Paket anhand der Informationen im Header analysiert, baut Stateful Inspection eine Statustabelle auf, um alle Verbindungen zu kontrollieren, welche sämtliche Schnittstellen der Firewall passieren, und sorgt dafür, dass diese gültig sind. Die Stateful Firewall des Vigor-Routers kontrolliert somit nicht nur die Header-Information, sondern auch den Verbindungsstatus.

DoS-Abwehr

Die Funktionalität der **DoS-Abwehr** ermöglicht die Erkennung und Entschärfung von DoS-Angriffen. Die Angriffe können entweder durch Überflutung (Flooding) stattfinden oder direkt auf Schwachstellen abzielen. Der Überflutungsansatz versucht, Ihre Systemressourcen komplett in Anspruch zu nehmen, während die eigentlichen Angriffe den Zweck verfolgen, die Schwachstellen des Protokolls oder des Betriebssystems auszunutzen.

Die **DoS-Abwehr**funktion ermöglicht dem Vigor-Router, jedes eingehende Paket anhand der Angriffssignaturdatenbank zu analysieren. Jedes bösartige Paket, das sich vervielfältigen könnte, um den Host im sicheren LAN lahmzulegen, wird grundsätzlich blockiert. Sofern Sie einen Syslog-Server eingerichtet haben, wird außerdem eine Syslog-Meldung versandt.

Der Vigor-Router beobachtet auch den Verkehr. Ungewöhnliche Verkehrsflüsse, welche vorher festgelegte Parameter wie die Anzahl der Schwellenwerte überschreiten, werden als Angriff gekennzeichnet. Der Vigor-Router aktiviert daraufhin seinen Abwehrmechanismus, um den Angriff in Echtzeit unschädlich zu machen.

Nachfolgend sind die Angriffsarten aufgeführt, die von der DoS/DDoS-Verteidigungsfunktion erkannt werden können:

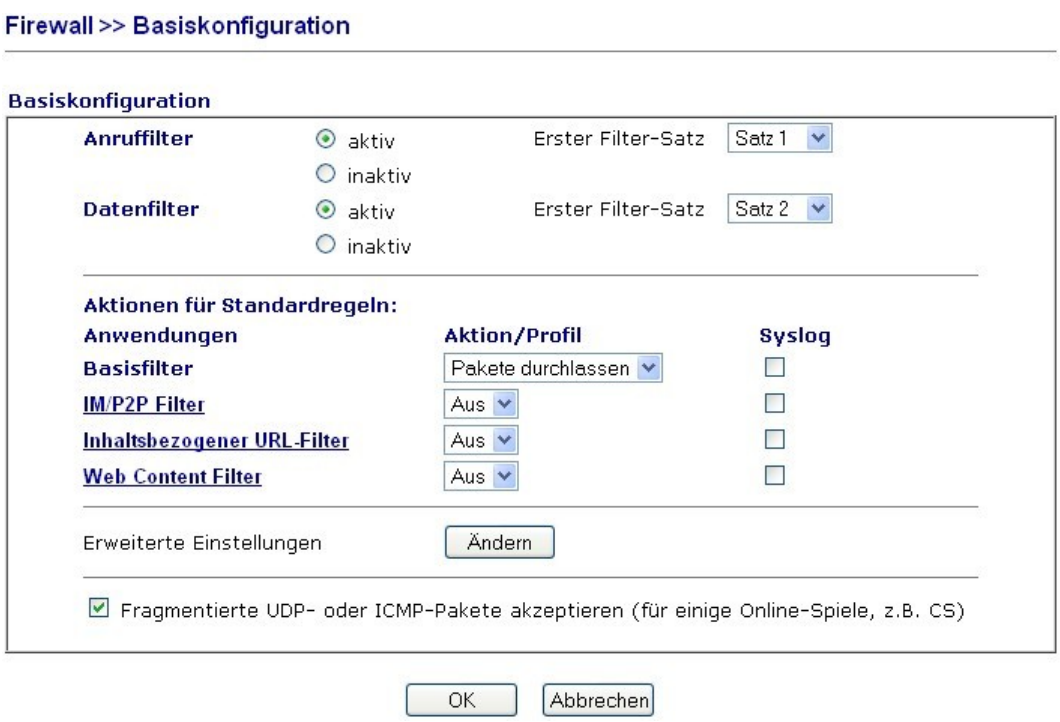
1. SYN Flood Angriff
2. UDP Flood Angriff
3. ICMP Flood Angriff
4. Port Scan Angriff
5. IP Options
6. Land-Angriff
7. Smurf-Angriff
8. Trace Route
9. SYN Fragmente
10. Fraggle-Angriff
11. TCP Flag Scan
12. Teardrop-Angriff
13. Ping of Death Angriff
14. ICMP Fragmente
15. Unbekanntes Protokoll

Die folgende Abbildung zeigt die Menüeinträge für Firewall:

5.4.2 Basiskonfiguration

Unter Basiskonfiguration können Sie die IP-Filtereinstellungen und andere allgemeine Optionen konfigurieren. **Anruffilter** und **Datenfilter** können hier aktiviert oder deaktiviert werden. Unter gewissen Voraussetzungen können Ihre Filter-Sätze so kombiniert werden, dass diese nacheinander abgearbeitet werden. Hier müssen Sie lediglich den **Ersten Filter-Satz** einstellen. Außerdem können Sie die **Log Flag**-Einstellungen konfigurieren und **Fragmentierte UDP-Pakete oder ICMP-Pakete** akzeptieren.

Wählen Sie **Firewall** und klicken Sie auf **Basiskonfiguration**, um die Seite mit den grundlegenden Einstellungen zu öffnen.



Anruffilter - Markieren Sie **Aktiv**, um die Anruffilterfunktion zu aktivieren. Wählen Sie den ersten Filter-Satz für den Anruffilter.

Datenfilter - Markieren Sie **Aktiv**, um die Datenfilterfunktion zu aktivieren. Wählen Sie den ersten Filter-Satz für den Datenfilter.

Aktion/Profil - Wählen Sie für die Pakete, die den Filterregeln nicht entsprechen, **Durchlassen** oder **Blockieren**.

IM/P2P-Filter - Wählen Sie eine der Profileinstellungen unter **IM/P2P Filter** (erstellt in **CSM>> IM/P2P Filter**), welche dieser Router anwenden soll. Richten Sie zunächst mindestens ein Profil zur Auswahl unter **CSM>> IM/P2P Filter** ein. Zur Fehlersuche können Sie die Vorgänge zum **IM/P2P Filter** aufzeichnen, indem Sie die Log-Funktion aktivieren. Die Meldungen werden an den Syslog-Server gesandt. Zu Einzelheiten sehen Sie bitte Abschnitt 5.14.5 **Syslog/Mail-Alarm**.

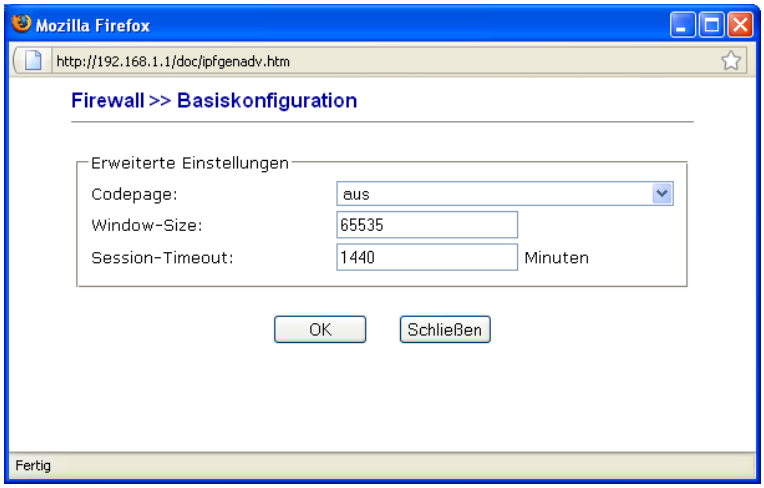
Inhaltsbezogener URL-Filter - Wählen Sie

eine der Profileinstellungen für den **inhaltsbezogenen URL-Filter** (erstellt in **CSM>> Inhaltsbezogener URL-Filter**), welche dieser Router anwenden soll. Richten Sie zunächst mindestens ein Profil zur Auswahl unter **CSM>> URL-Filter** ein. Zur Fehlersuche können Sie die Vorgänge zum inhaltsbezogenen URL-Filter aufzeichnen, indem Sie die Log-Funktion aktivieren. Die Meldungen werden an den Syslog-Server gesandt. Weitere Einzelheiten finden Sie im Abschnitt 5.14.5 **Syslog/Mail-Alarm**.

Inhaltsbezogener Web-Filter - Wählen Sie eine der Profileinstellungen für den **inhaltsbezogenen Web-Filter** (erstellt in **CSM>> Inhaltsbezogener Web-Filter**), welche dieser Router anwenden soll. Richten Sie zunächst mindestens ein Profil zur Auswahl unter **CSM>> Inhaltsbezogener Web-Filter** ein. Zur Fehlersuche können Sie die Vorgänge zum **inhaltsbezogenen Web-Filter** aufzeichnen, indem Sie die Log-Funktion aktivieren. Die Meldungen werden an den Syslog-Server gesandt. Zu Einzelheiten sehen Sie bitte Abschnitt 5.14.5 **Syslog/Mail-Alarm**.

Syslog - Zur Fehlersuche können Sie das Filter-Log und/oder das CSM-Log durch Anhaken des Kästchens aktivieren. Das Log wird im DrayTek Syslog-Fenster angezeigt.

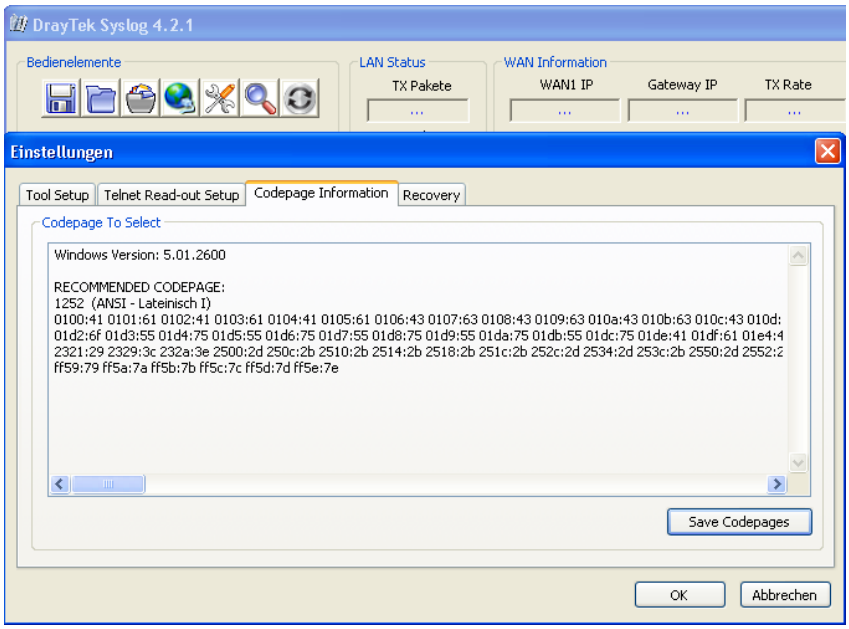
Erweiterte Einstellungen - Klicken Sie auf **Bearbeiten**, um das folgende Fenster zu öffnen. Es wird jedoch **dringend empfohlen**, hier die Standardeinstellungen zu verwenden.



Codepage - Diese Funktion wird verwendet, um die Zeichen verschiedener Sprachen zu vergleichen. Die Auswahl der korrekten Codepage ermöglicht dem System, die Daten der URL in korrekte ASCII-Zeichen umzuwandeln und die Treffsicherheit des inhaltsbezogenen URL-Filters zu verbessern.

Die Standardeinstellung ist ANSI 1252 Latin I. Falls Sie keine Codepage wählen, werden URLs nicht umgewandelt. Bitte wählen Sie eine Codepage aus der Dropdown-Liste.

Falls Sie sich nicht sicher sind, welche Codepage zu wählen ist, öffnen Sie bitte Syslog. Die empfohlene Codepage ist im Reiter Codepage-Information des Konfigurationsdialogs aufgeführt.



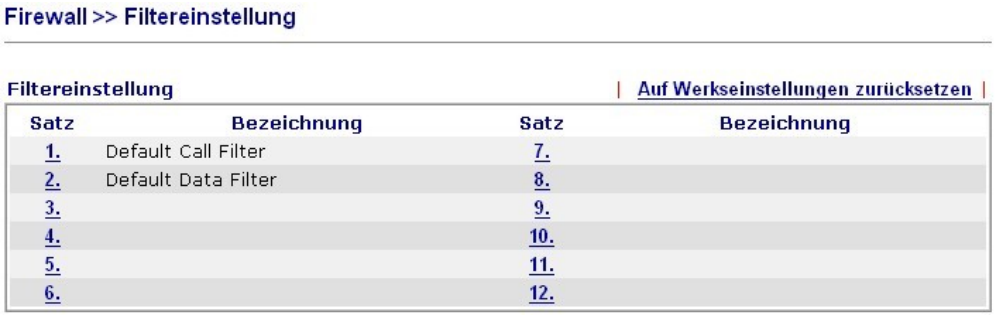
Window-Size – Bestimmt die Größe des TCP-Protokolls (0~65535). Je größer der Wert ist, desto besser wird die Leistung sein. Falls das Netzwerk jedoch nicht stabil ist, ist ein kleiner Wert geeigneter.

Session-Timeout – Die Einstellung einer maximalen Dauer für Sitzungen ermöglicht die bestmögliche Nutzung der Netzwerkressourcen. Der Queue-Timeout gilt lediglich für das TCP-Protokoll, der Session-Timeout wird für den Datenfluss konfiguriert, welcher der Firewall-Regel entspricht.

Einige Online-Spiele (z.B. Half Life) verwenden eine Vielzahl von fragmentierten UDP-Paketen, um Game-Daten zu übermitteln. Als sichere Firewall verwirft der Vigor-Router diese fragmentierten Pakete normalerweise, um Angriffe zu vermeiden, es sei denn, Sie aktivieren **Fragmentierte UDP-Pakete akzeptieren.** Wenn dieses Kästchen angehakt ist, können Sie solche Online-Spiele spielen. Falls Sicherheitsbedenken schwerer wiegen, aktivieren Sie **Fragmentierte UDP-Pakete akzeptieren** lieber nicht.

5.4.3 Filtereinstellung

Klicken Sie auf **Firewall** und wählen Sie **Filtereinstellung**, um die Konfigurationsseite zu öffnen.



Um einen Filter zu bearbeiten oder hinzuzufügen, klicken Sie auf die entsprechende Satznummer. Die folgende Seite erscheint. Jeder Filter-Satz kann bis zu sieben Regeln enthalten. Klicken Sie auf die Taste mit der Regelnummer, um die entsprechende Regel zu bearbeiten. Markieren Sie das Kästchen **Aktiv**, um die Regel zu aktivieren.

Firewall >> Filtereinstellung >> Filter-Satz ändern
Filter-Satz 1
Beschreibung: Default Call Filter
Filterregel Aktiv Bezeichnung Aufwerten Abwerten
1 Block NetBios nach unten
2 nach oben nach unten
3 nach oben nach unten
4 nach oben nach unten
5 nach oben nach unten
6 nach oben nach unten
7 nach oben
Nächster Filter-Satz keiner
OK Löschen Abbrechen

Filterregel - Klicken Sie auf eine der Nummern (1 ~ 7), um die entsprechende Filterregel zu bearbeiten. Der Dialog Filterregeln ändern erscheint. Die folgende Seite enthält detaillierte Informationen.

Aktiv - Filterregel aktivieren oder deaktivieren.

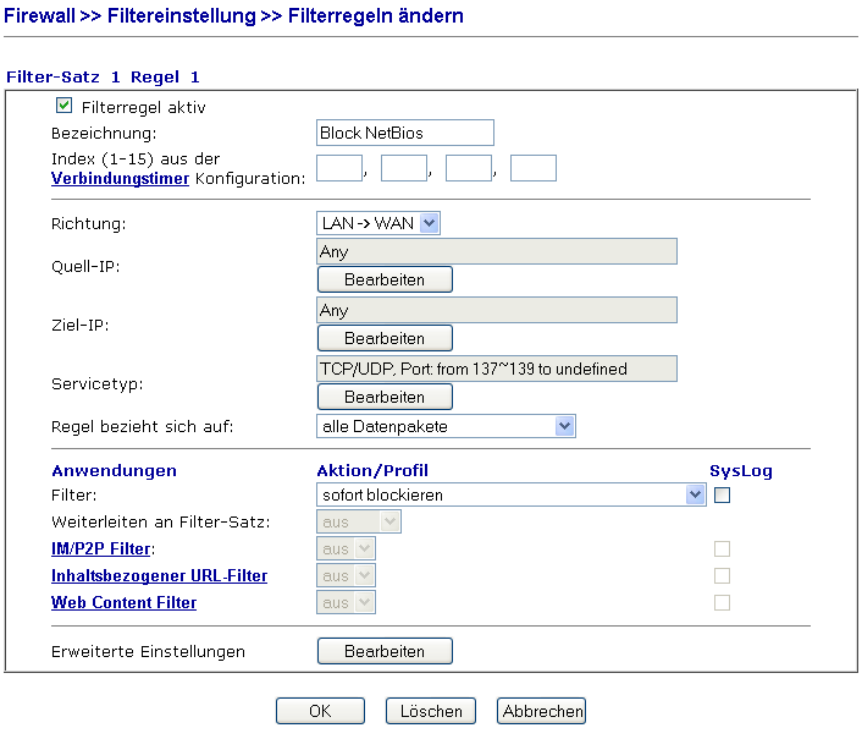
Bezeichnung - Geben Sie eine Bezeichnung für den Filter-Satz ein. Die maximale Länge beträgt 23 Zeichen.

Aufwerten/Abwerten - Klicken Sie auf **Nach oben** oder **Nach unten**, um die Reihenfolge der Filterregeln zu ändern.

Nächster Filter-Satz - Setzen Sie den Link auf den nächsten Filter-Satz, der nach dem aktuellen Filter ausgeführt werden soll. Vermeiden Sie Ketten mit zu vielen Filter-Sätzen.

Um eine **Filterregel** zu bearbeiten, klicken Sie auf die Indexnummer der **Filterregel**, wodurch

Sie auf die Konfigurationsseite für die **Filterregel** gelangen.



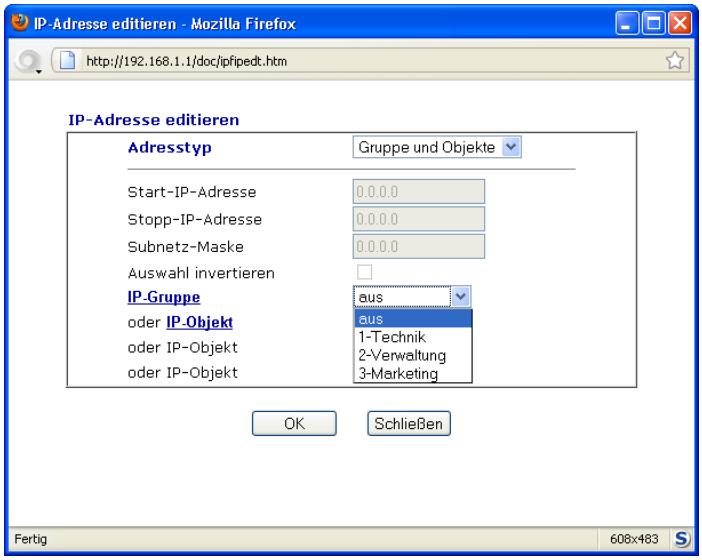
Filterregel aktiv - Markieren Sie dieses Kästchen, um die Filterregel zu aktivieren.

Beschreibung - Geben Sie eine Bezeichnung für den Filter-Satz ein. Die maximale Länge beträgt 14 Zeichen.

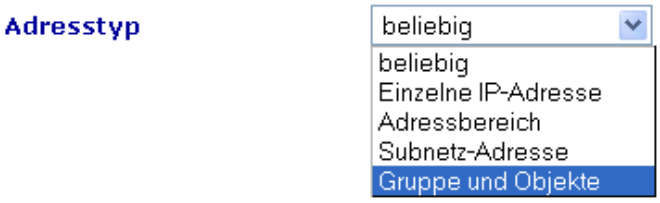
Index (1-15) - Sie können die LAN-PCs so konfigurieren, dass sie lediglich in gewissen Zeitabschnitten in Betrieb sind. Sie können bis zu vier der 15 vordefinierten Timer unter **Anwendungen >> Timer** wählen. Per Standardeinstellung ist dieses Feld leer, und die Funktion ist ständig in Betrieb.

Richtung - Stellen Sie die Paketflussrichtung ein (LAN->WAN/WAN->LAN). Dies gilt nur für den **Datenfilter**. Beim **Anruffilter** gilt diese Einstellung nicht, da sich dieser lediglich auf den ausgehenden Verkehr bezieht.

Quell-/Ziel-IP - Klicken Sie auf **Bearbeiten**, um in den folgenden Dialog zu gelangen, in dem Sie die Quell-/Ziel-IP oder IP-Bereiche wählen können.

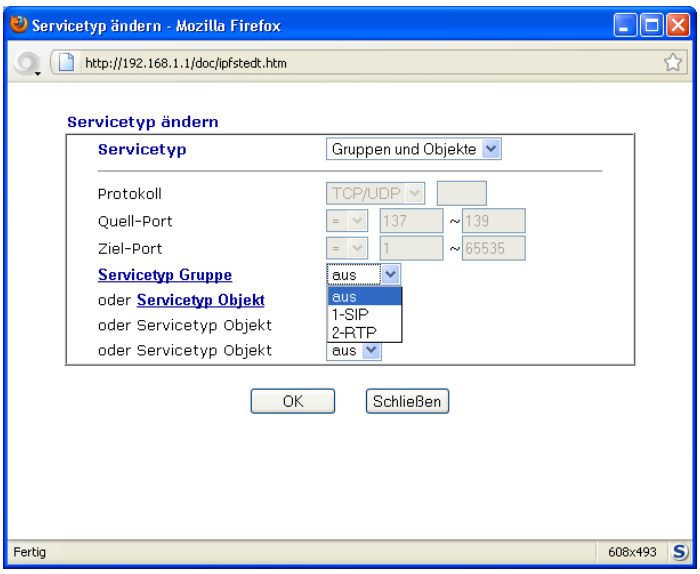


Um die IP-Adresse manuell einzustellen, wählen Sie bitte als Adresstyp **Beliebige Adresse/Einzelne Adresse/Adressbereich/Subnetz-Adresse** und geben sie in diesem Dialog ein. Falls Sie außerdem den IP-Bereich bestimmter Gruppen oder Objekte verwenden möchten, wählen Sie bitte als Adresstyp **Gruppen und Objekte**.



Aus der Dropdown-Liste **IP-Gruppe** wählen Sie diejenige, die Sie anwenden möchten. Alternativ können Sie die Dropdown-Liste **IP-Objekt** benutzen, um das gewünschte Objekt zu wählen.

Servicetyp - Klicken Sie auf **Bearbeiten**, um in den folgenden Dialog zu gelangen, in dem Sie einen geeigneten Servicetyp wählen können.



Um den Servicetyp manuell einzustellen, wählen Sie bitte **Benutzerdefiniert** als Servicetyp und geben ihn in diesem Dialog ein. Falls Sie außerdem den Servicetyp bestimmter Gruppen oder Objekte verwenden möchten, wählen Sie bitte als Servicetyp **Gruppen und Objekte**.

Protokoll - Geben Sie das/die Protokoll(e) an, auf welche(s) diese Filterregel anzuwenden ist.

Quell-/Ziel-Port -

(=) – Identische erste und letzte Werte weisen auf einen einzelnen Port hin; unterschiedliche erste und letzte Werte weisen auf einen Portbereich hin, der für diesen Servicetyp verfügbar ist.

(!=) – Identische erste und letzte Werte weisen auf alle Ports außer dem hier angegebenen Port hin; unterschiedliche erste und letzte Werte weisen darauf hin, dass alle Ports außer dem hier angegebenen Bereich für diese Servicetyp verfügbar sind.

(>) – Die Portnummer, die größer als dieser Wert ist, ist verfügbar.

(<) – Die Portnummer, die kleiner als dieser Wert ist, ist für dieses Profil verfügbar.

Servicetyp Gruppe/Objekt - Verwenden Sie die Dropdown-Liste, um Ihre Auswahl zu treffen.

Fragmente - Bestimmen Sie die Aktion für fragmentierte Pakete. Dies gilt lediglich für den **Datenfilter**.

***Alle Datenpakete* -** Keine Aktion für

fragmentierte Pakete.

Alle nicht fragmentierten Pakete - Regel auf nicht fragmentierte Pakete anwenden.

Alle fragmentierten Pakete - Regel auf fragmentierte Pakete anwenden.

Alle Fragmente ohne Header - Regel nur auf Pakete anwenden, die zu kurz sind, um einen vollständigen Header zu enthalten.

Basisfilter - Gibt die durchzuführende Aktion an, wenn Pakete der Regel entsprechen.

Sofort blockieren - Pakete, die mit der Regel übereinstimmen, werden sofort verworfen.

Sofort durchlassen - Pakete, die mit der Regel übereinstimmen, werden sofort durchgelassen.

Blockieren, falls keine weitere Übereinstimmung - Pakete, die mit der Regel übereinstimmen und mit keinen weiteren Regeln übereinstimmen, werden verworfen.

Durchlassen, falls keine weitere Übereinstimmung - Pakete, die mit der Regel übereinstimmen und mit keinen weiteren Regeln übereinstimmen, werden durchgelassen.

Weiterleiten an Filter-Satz - Falls das Paket der Filterregel entspricht, leitet die nächste Filterregel das Paket zum angegebenen Filter-Satz weiter. Wählen Sie die nächste Filterregel aus dem Dropdown-Menü. Vergessen Sie nicht, dass der Router die angegebene Filterregel ständig anwenden wird und nicht mehr zur vorherigen Filterregel zurückkehren wird.

IM/P2P-Filter - Wählen Sie eine der Profileinstellungen unter **IM/P2P Filter** (erstellt in **CSM>> IM/P2P Filter**), welche dieser Router anwenden soll. Richten Sie zunächst mindestens ein Profil zur Auswahl unter **CSM>> IM/P2P Filter** ein. Zur Fehlersuche können Sie die Vorgänge zum **IM/P2P Filter** aufzeichnen, indem Sie die Log-Funktion aktivieren. Die Meldungen werden an den Syslog-Server gesandt. Zu Einzelheiten sehen Sie bitte Abschnitt 5.14.5 **Syslog/Mail-Alarm**.

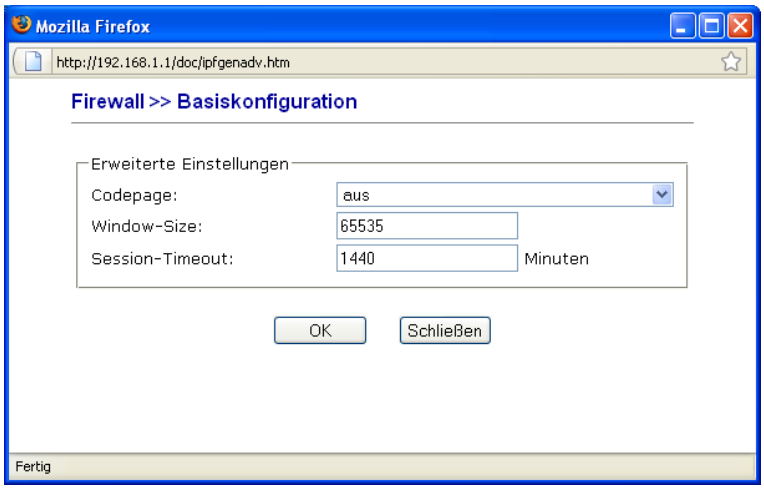
Inhaltsbezogener URL-Filter - Wählen Sie eine der Profileinstellungen für den **inhaltsbezogenen URL-Filter** (erstellt in **CSM>> Inhaltsbezogener URL-Filter**), welche dieser Router anwenden soll. Richten Sie zunächst mindestens ein Profil zur Auswahl unter **CSM>> URL-Filter** ein. Zur Fehlersuche können Sie die Vorgänge zum inhaltsbezogenen URL-Filter aufzeichnen, indem Sie die Log-Funktion aktivieren. Die Meldungen werden an den Syslog-Server gesandt. Zu Einzelheiten

sehen Sie bitte Abschnitt 5.14.5 **Syslog/Mail-Alarm**.

Inhaltsbezogener Web-Filter - Wählen Sie eine der Profileinstellungen für den **inhaltsbezogenen Web-Filter** (erstellt in **CSM>> Inhaltsbezogener Web-Filter**), welche dieser Router anwenden soll. Richten Sie zunächst mindestens ein Profil zur Auswahl unter **CSM>> Inhaltsbezogener Web-Filter** ein. Zur Fehlersuche können Sie die Vorgänge zum **inhaltsbezogenen Web-Filter** aufzeichnen, indem Sie die Log-Funktion aktivieren. Die Meldungen werden an den Syslog-Server gesandt. Zu Einzelheiten sehen Sie bitte Abschnitt 5.14.5 **Syslog/Mail-Alarm**.

SysLog - Zur Fehlersuche können Sie hier das Filter-Log und/oder das CSM-Log aktivieren. Markieren Sie das entsprechende Kästchen, um die Log-Funktion zu aktivieren. Daraufhin wird das Filter-Log und/oder CSM-Log im DrayTek Syslog-Fenster angezeigt.

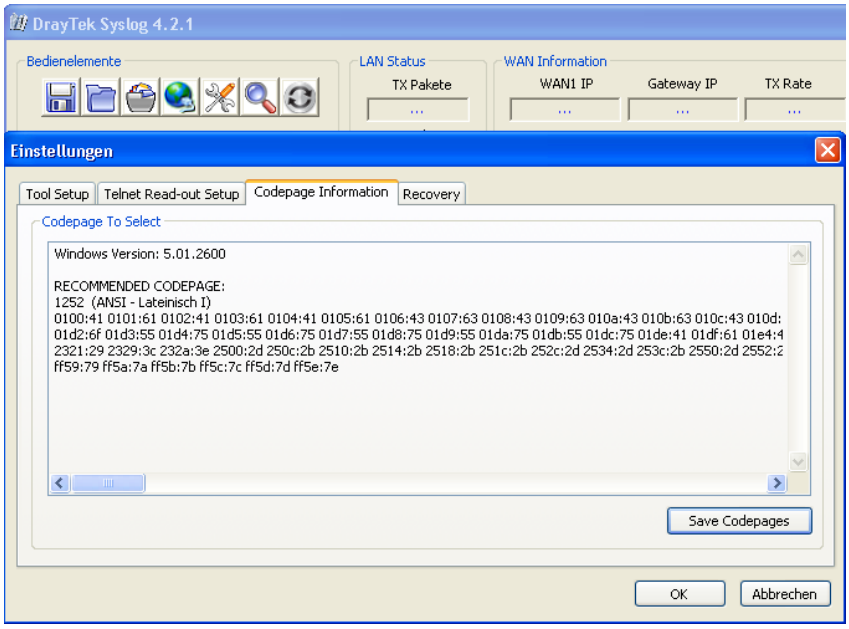
Erweiterte Einstellungen - Klicken Sie auf **Bearbeiten**, um das folgende Fenster zu öffnen. Es wird jedoch **dringend empfohlen**, hier die Standardeinstellungen zu verwenden.



Codepage - Diese Funktion wird verwendet, um die Zeichen verschiedener Sprachen zu vergleichen. Die Auswahl der korrekten Codepage ermöglicht dem System, die Daten der URL in korrekte ASCII-Zeichen umzuwandeln und die Treffsicherheit des inhaltsbezogenen URL-Filters zu verbessern. Die Standardeinstellung ist ANSI 1252 Latin I. Falls Sie keine Codepage wählen, werden URLs nicht umgewandelt. Bitte wählen Sie eine Codepage aus der Dropdown-Liste.

Falls Sie sich nicht sicher sind, welche Codepage zu wählen ist, öffnen Sie bitte Syslog. Die empfohlene Codepage ist im Reiter

Codepage-Information des Konfigurationsdialogs aufgeführt.

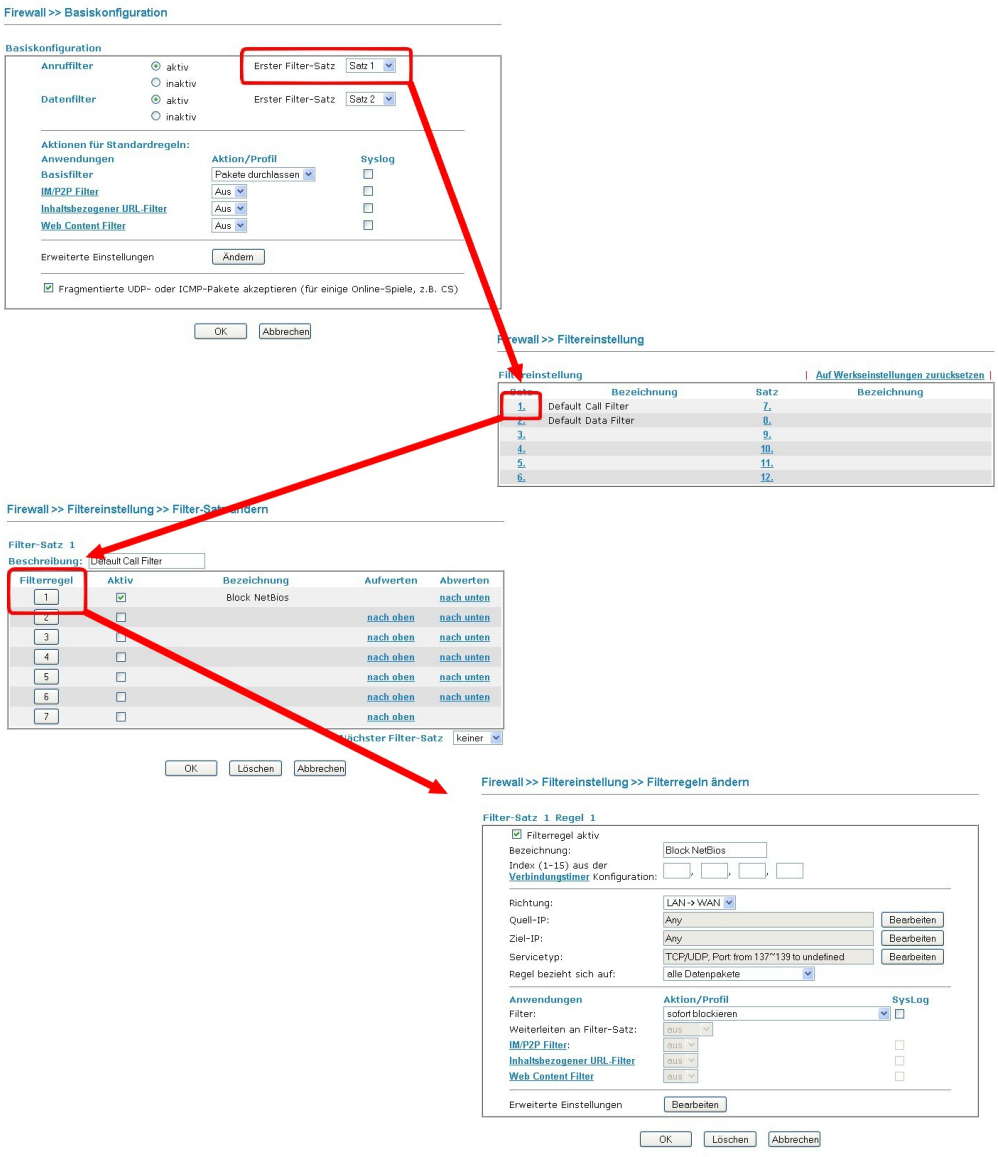


Window-Size – Bestimmt die Größe des TCP-Protokolls (0~65535). Je größer der Wert ist, desto besser wird die Leistung sein. Falls das Netzwerk jedoch nicht stabil ist, ist ein kleiner Wert geeigneter.

Session-Timeout – Die Einstellung einer maximalen Dauer für Sitzungen ermöglicht die bestmögliche Nutzung der Netzwerkressourcen. Der Queue-Timeout gilt lediglich für das TCP-Protokoll, der Session-Timeout wird für den Datenfluss konfiguriert, welcher der Firewall-Regel entspricht.

Beispiel

Wie bereits erwähnt, wird der gesamte Verkehr mit Hilfe von zwei IP-Filtern aufgeteilt und vermittelt: Anruffilter oder Datenfilter. Sie können unter **Filtereinstellung** bis zu zwölf Anruffilter und Datenfilter einrichten und diese sogar seriell kombinieren. Jeder Filter-Satz besteht aus sieben Filterregeln, die näher definiert werden können. Danach können Sie in der **Basiskonfiguration** einen Satz als zuerst anzuwendenden Anruffilter oder Datenfilter bestimmen.



5.4.4 DoS-Abwehr

Als Subfunktionalität der IP-Filter/Firewall gibt es 15 Arten von Erkennungs-/Abwehrfunktionen in der Konfiguration der **DoS-Abwehr**. Die DoS-Abwehrfunktionalität ist standardmäßig deaktiviert.

Wählen Sie **Firewall** und klicken auf **DoS-Abwehr**, um die Konfigurationsseite zu öffnen.

Aktiv - Markieren Sie das Kästchen, um die DoS-Abwehrfunktionalität zu aktivieren.

Aktiviere SYN Flood Abwehr - Markieren Sie das Kästchen, um die SYN Flood Abwehrfunktion zu aktivieren. Sobald der Schwellenwert der TCP SYN Pakete aus dem Internet den definierten Wert überschreitet, beginnt der Vigor-Router, die folgenden TCP SYN Pakete, die über dem unter Timeout definierten Zeitraum liegen, zufällig zu verwerfen. Der Zweck dieser Vorgehensweise ist, zu vermeiden, dass die TCP SYN Pakete die begrenzten Ressourcen des Vigor-Routers ausschöpfen. Standardmäßig wird der Schwellenwert auf 50 Pakete pro Sekunde und der Timeout auf 10 Sekunden gesetzt.

Aktiviere UDP Flood Abwehr - Markieren Sie das Kästchen, um die UDP Flood Abwehrfunktion zu aktivieren. Sobald der Schwellenwert der UDP-Pakete aus dem Internet den definierten Wert überschreitet, beginnt der Vigor-Router, die folgenden UDP-Pakete, die über dem unter Timeout definierten Zeitraum liegen, zufällig zu verwerfen. Standardmäßig werden der Schwellenwert auf 150 Pakete pro Sekunde und der Timeout auf 10 Sekunden gesetzt.

Aktiviere ICMP Flood Abwehr - Markieren Sie das Kästchen, um die ICMP Flood Abwehrfunktion zu aktivieren. Ähnlich wie bei der UDP Flood Abwehrfunktion verwirft der Router daraufhin die aus dem Internet kommenden ICMP-Echo-Requests, sobald der Schwellenwert der ICMP-Pakete aus dem Internet den definierten Wert überschreitet. Standardmäßig werden der Schwellenwert auf 50 Pakete pro Sekunde und der Timeout auf 10 Sekunden gesetzt.

Aktiviere Port Scan Abwehr - Bei Port Scan Angriffen auf den Vigor-Router werden viele Pakete an viele Ports gesandt, um eine Antwort von bestimmten Diensten zu erhalten. Markieren Sie das Kästchen, um die Port Scan Erkennung zu aktivieren. Jedes Mal, wenn dieses bösartige Suchverhalten erkannt wird, was durch Überwachung des Port Scan Schwellenwertes geschieht, versendet der Vigor-Router eine Warnung. Standardmäßig beträgt der Schwellenwert des Vigor-Routers 150 Pakete pro Sekunde.

IP-Options blockieren - Markieren Sie das Kästchen, um die Funktion zum Blockieren von IP-Options zu aktivieren. Der Vigor-Router wird somit jegliche IP-Pakete mit IP-Option-Feld im Datagramm-Header ignorieren. Der Grund für die Beschränkung von IP-Options besteht darin, wichtige Informationen wie Sicherheits- und TCC-Parameter (geschlossene Benutzergruppe), eine Reihe von Internet-Adressen, Routing-Meldungen usw. nicht weiterzugeben. Ein Außenstehender könnte sonst Einzelheiten über Ihre privaten Netzwerke in Erfahrung bringen.

Land blockieren - Markieren Sie das Kästchen, damit der Vigor-Router Land-Attacken abwehrt. Die Land-Attacke verbindet die Technologie der SYN-Angriffe mit IP-Spoofing. Eine Land-Attacke findet statt, wenn ein Angreifer gefälschte SYN-Pakete, bei denen die Quell- und Zieladressen sowie die Portnummer identisch sind, an potentielle Opfer sendet.

Smurf blockieren - Markieren Sie das Kästchen, um die Funktion zum Blockieren von Smurf zu aktivieren. Der Vigor-Router wird daraufhin jegliche ICMP-Echo-Requests an die Broadcast-Adresse ignorieren.

Trace Route blockieren - Markieren Sie das Kästchen, damit der Vigor-Router keine Trace Route Pakete weiterleitet.

SYN Fragmente blockieren - Markieren Sie das Kästchen, um die Funktion zum Blockieren von SYN-Fragmenten zu aktivieren. Der Vigor-

Router wird daraufhin jegliche Pakete verwerfen, bei denen das SYN-Flag gesetzt ist und die zusätzliche Bit-Fragmente haben.

Fraggle Attack blockieren - Markieren Sie das Kästchen, um die Funktion zum Blockieren von Fraggle-Attacken zu aktivieren. Jegliche aus dem Internet erhaltene UDP-Pakete an die Broadcast-Adresse werden blockiert.

Die Aktivierung der DoS/DDoS-Abwehrfunktionalität kann unter Umständen auch gültige Pakete blockieren. Wenn Sie zum Beispiel die Abwehr von Fraggle-Attacken aktivieren, werden alle aus dem Internet kommenden UDP-Pakete an die Broadcast-Adresse blockiert. Folglich können auch die RIP-Pakete aus dem Internet verworfen werden.

TCP Flag Scan blockieren - Markieren Sie das Kästchen, um die Funktion zum Blockieren von TCP Flag Scan zu aktivieren. Jegliche TCP-Pakete mit anormal gesetzten Flags werden verworfen. Diese Scan-Aktivitäten umfassen *Null Scan*, *FIN ohne ACK Scan*, *SYN FIN Scan*, *Xmas Scan* und *Full Xmas Scan*.

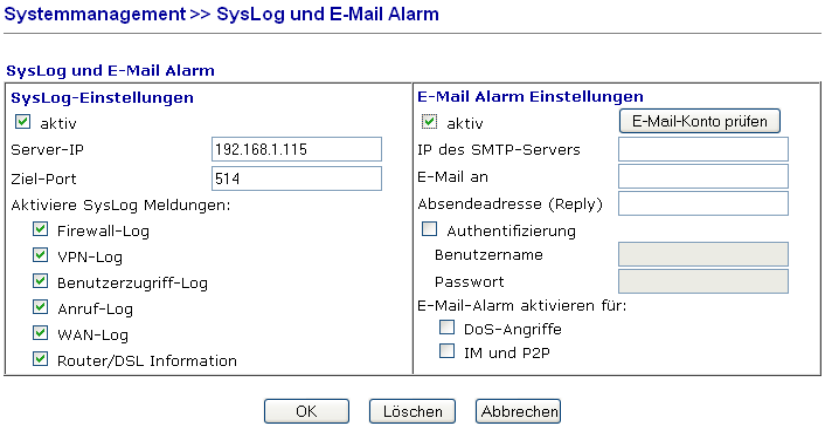
Tear Drop blockieren - Markieren Sie das Kästchen, um die Funktion zum Blockieren von Tear Drop zu aktivieren. Viele Rechner können abstürzen, wenn sie ICMP-Datagramme (Pakete) erhalten, welche die maximale Länge überschreiten. Um diese Art von Angriffen zu vermeiden, hat der Vigor-Router die Fähigkeit, fragmentierte ICMP-Pakete mit einer Länge von mehr als 1024 Oktetten zu verwerfen.

Ping of Death blockieren - Markieren Sie das Kästchen, um die Funktion zum Blockieren von Ping of Death zu aktivieren. Bei dieser Art von Angriffen sendet der Angreifer überlappende Pakete an die Ziel-Hosts, damit diese hängen bleiben, wenn sie die Pakete wieder zusammensetzen. Der Vigor-Router wird jegliche Pakete blockieren, bei welchen diese Angriffsaktivität festgestellt wird.

ICMP Fragment blockieren - Markieren Sie das Kästchen, um die Blockierfunktion für ICMP-Fragmente zu aktivieren.

Unbekannte Protokolle blockieren - Markieren Sie das Kästchen, um die Funktion zum Blockieren von unbekannten Protokollen zu aktivieren. Einzelne IP-Pakete haben im Datagramm-Header ein Protokollfeld, in dem der Protokolltyp angegeben wird. Protokolltypen über 100 sind jedoch reserviert und bis jetzt undefiniert. Daher sollte der Router in der Lage sein, diese Art von Paketen zu erkennen und abzulehnen.

Warnmeldungen - Die Syslog-Funktion ermöglicht die Annahme von Meldungen vom Vigor-Router. Der Benutzer als Syslog-Server erhält die Meldungen vom Vigor-Router, dem Syslog-Client.



Sämtliche mit der **DoS-Abwehr** zusammenhängenden Warnmeldungen werden an den Benutzer gesandt, der sie über den Syslog-Daemon kontrollieren kann. Suchen Sie in der Meldung nach dem Schlüsselwort **DoS**, gefolgt von einer Bezeichnung, welche die Art von erkannten Angriffen bestimmt.

5.5 Objekte

IP-Bereiche und Port-Bereiche, auf welche eine bestimmte Router-Konfiguration angewendet werden soll, können als ***Objekte*** definiert werden, die zwecks vereinfachter Handhabung als ***Gruppen*** zusammengefasst werden können. Daraufhin steht das entsprechende Objekt/die Gruppe für die Anwendung der Einstellungen zur Auswahl. Es können beispielsweise alle IPs einer Abteilung als IP-Objekt (IP-Adressbereich) definiert werden.

5.5.1 IP-Objekt

Sie können bis zu 192 IP-Objekte mit unterschiedlichen Bedingungen einrichten.

Objekte >> IP-Objekt

Profile der IP-Objekte: | Auf Werkseinstellungen zurücksetzen |

Index	Name	Index	Name
1.		17.	
2.		18.	
3.		19.	
4.		20.	
5.		21.	
6.		22.	
7.		23.	
8.		24.	
9.		25.	
10.		26.	
11.		27.	
12.		28.	
13.		29.	
14.		30.	
15.		31.	
16.		32.	

<< 1-32 | 33-64 | 65-96 | 97-128 | 129-160 | 161-192 >> Weiter >>

Auf Werkseinstellungen zurücksetzen Alle Profile löschen.

Klicken Sie auf die Nummer in der Indexspalte, um zu den Detaileinstellungen zu gelangen.

Name - Geben Sie für dieses Profil eine Bezeichnung ein. Es können bis zu 15 Zeichen eingegeben werden.

SchnittstelleWählen Sie eine Schnittstelle (WAN, LAN, oder Beliebig).

Die Einstellung **Richtung** unter **Filterregeln ändern** ermöglicht Ihnen beispielsweise die Angabe einer IP-Adresse oder eines IP-Bereichs für das WAN oder LAN oder irgendeine IP-Adresse. Falls Sie hier als **Schnittstelle** LAN angeben und LAN als Richtung unter **Filterregeln ändern** wählen, werden alle mit der LAN-Schnittstelle angegebenen IP-Adressen zur Auswahl auf der Seite **Filterregeln ändern** angeboten.

Adresstyp - Bestimmen Sie den Adresstyp der IP-Adresse.

Wählen Sie **Einzelne Adresse**, falls dieses Objekt nur eine einzelne IP-Adresse enthält.

Wählen Sie **Adressbereich**, falls dieses Objekt mehrere IP-Adressen innerhalb eines Bereichs beinhaltet.

Wählen Sie **Subnetz-Adresse**, falls dieses Objekt ein Subnetz für IP-Adressen enthält.

Wählen Sie **Beliebige Adresse**, falls dieses Objekt eine beliebige IP-Adresse enthält.

Start-IP-Adresse - Geben Sie eine einzelne IP-Adresse bzw. die Start-IP-Adresse eines Adressbereichs ein.

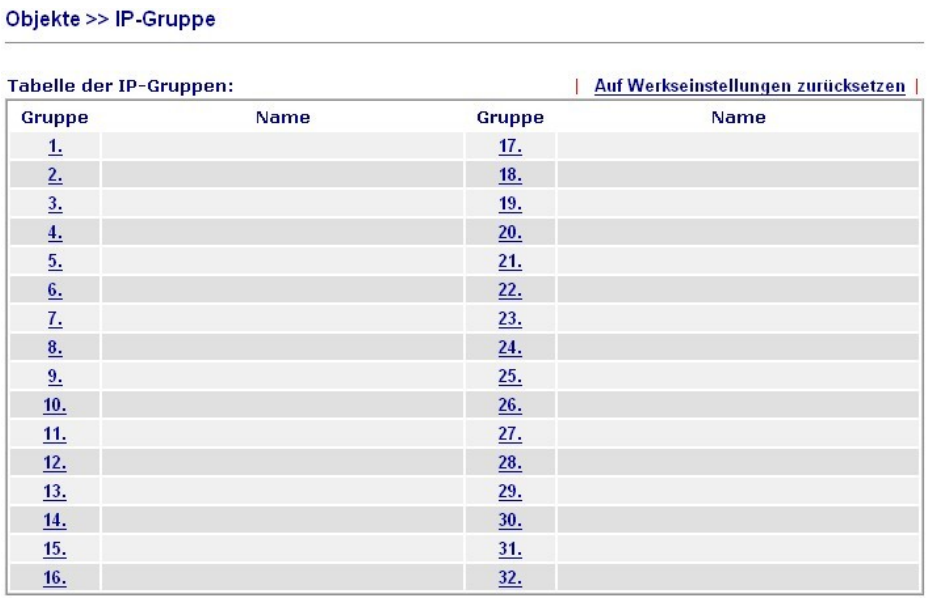
Stopp-IP-Adresse - Geben Sie die Stopp-IP-Adresse des Adressbereichs ein.

Subnetz-Maske - Geben Sie die Subnetz-Maske ein, falls als Typ Subnetz-Adresse gewählt wurde.

Auswahl invertieren - Falls dieses Kästchen markiert wird, werden alle außer den oben aufgeführten IP-Adressen ausgewählt.

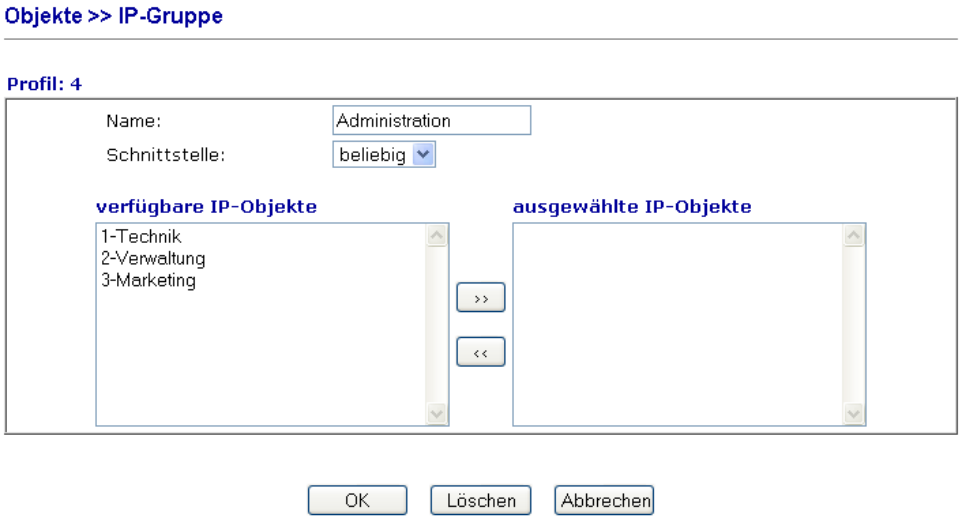
5.5.2 IP-Gruppe

Diese Seite ermöglicht Ihnen, mehrere IP-Objekte zu einer IP-Gruppe zu verbinden.



Auf Werkseinstellungen zurücksetzen Alle Profile löschen.

Klicken Sie auf die Nummer in der Indexspalte, um zu den Detaileinstellungen zu gelangen.



Name - Geben Sie für dieses Profil eine Bezeichnung ein. Es können bis zu 15 Zeichen eingegeben werden.

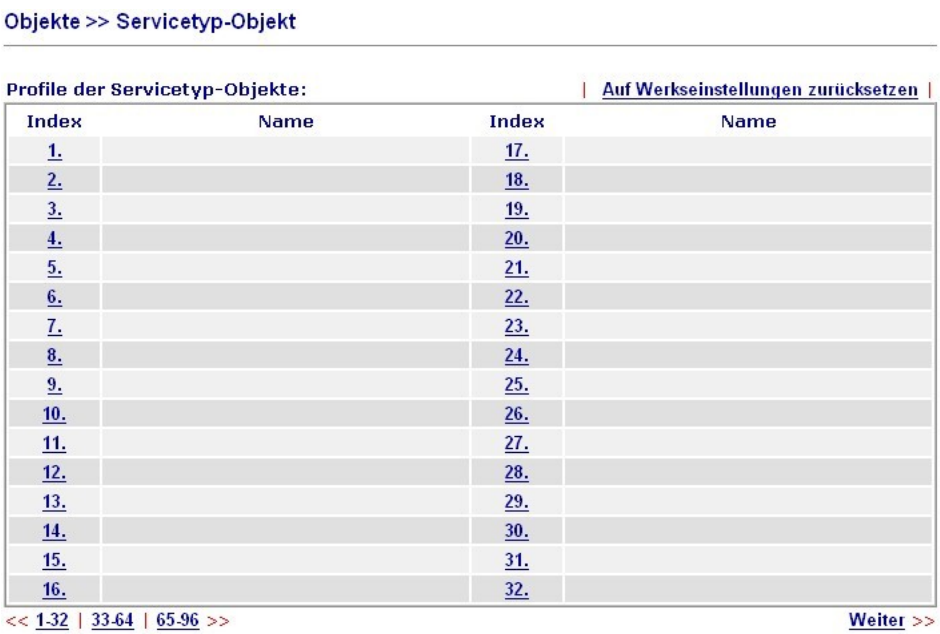
Schnittstelle - Wählen Sie WAN, LAN oder Beliebig, damit alle vorhandenen IP-Objekte mit der angegebenen Schnittstelle angezeigt werden.

Verfügbare IP-Objekte - Sämtliche vorhandene IP-Objekte mit der oben gewählten Schnittstelle werden in diesem Feld angezeigt.

Gewählte IP-Objekte - Klicken Sie auf die Taste >>, um die ausgewählten IP-Objekte in diesem Feld hinzuzufügen.

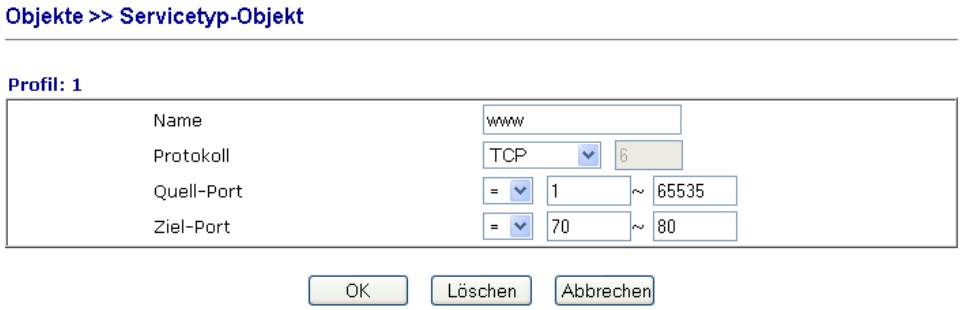
5.5.3 Servicetyp-Objekt

Sie können bis zu 96 Servicetyp-Objekte mit unterschiedlichen Bedingungen einrichten.



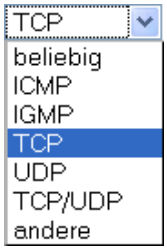
Auf Werkseinstellungen zurücksetzen Alle Profile löschen.

Klicken Sie auf die Nummer in der Indexspalte, um zu den Detaileinstellungen zu gelangen.



Name - Geben Sie für dieses Profil eine Bezeichnung ein.

Protokoll - Geben Sie das/die Protokoll(e) an, auf welche(s) dieses Profil anzuwenden ist.



Quell-/Ziel-Port - Die Spalten **Quellport** und **Zielport** werden für das TCP/UDP-Protokoll benötigt. Bei anderen Protokollen können diese Spalten ignoriert werden. Die Filterregel kann eine beliebige Portnummer ausfiltern.

(=) – Identische erste und letzte Werte weisen auf einen einzelnen Port hin; unterschiedliche erste und letzte Werte weisen auf einen Portbereich hin, der für dieses Profil verfügbar ist.

(!=) – Identische erste und letzte Werte weisen auf alle Ports außer dem hier angegebenen Port hin; unterschiedliche erste und letzte Werte weisen darauf hin, dass alle Ports außer dem hier angegebenen Bereich für diese Servicetyp verfügbar sind.

(>) – Die Portnummer, die größer als dieser Wert ist, ist verfügbar.

(<) – Die Portnummer, die kleiner als dieser Wert ist, ist für dieses Profil verfügbar.

Beispiel für Einstellungen eines Servicetyp-Objekts:

Profile der Servicetyp-Objekte:

Index	Name
1.	WWW
2.	SIP
3.	

5.5.4 Servicetyp-Gruppe

Diese Seite ermöglicht Ihnen, mehrere Servicetypen zu einer Gruppe zu verbinden.

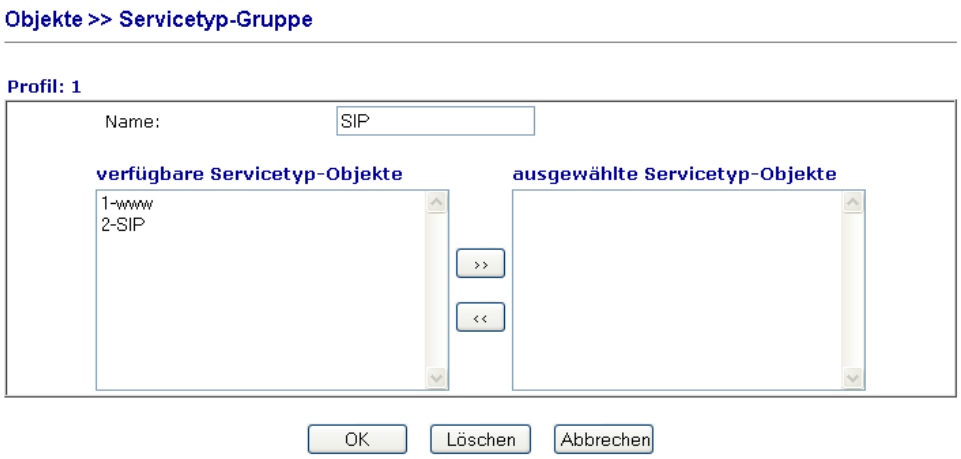
Objekte >> Servicetyp-Gruppe

Tabelle der Servicetyp-Gruppen: | Auf Werkseinstellungen zurücksetzen |

Gruppe	Name	Gruppe	Name
1.	SIP	17.	
2.	RTP	18.	
3.		19.	
4.		20.	
5.		21.	
6.		22.	
7.		23.	
8.		24.	
9.		25.	
10.		26.	
11.		27.	
12.		28.	
13.		29.	
14.		30.	
15.		31.	
16.		32.	

Auf Werkseinstellungen zurücksetzen Alle Profile löschen.

Klicken Sie auf die Nummer in der Indexspalte, um zu den Detaileinstellungen zu gelangen.



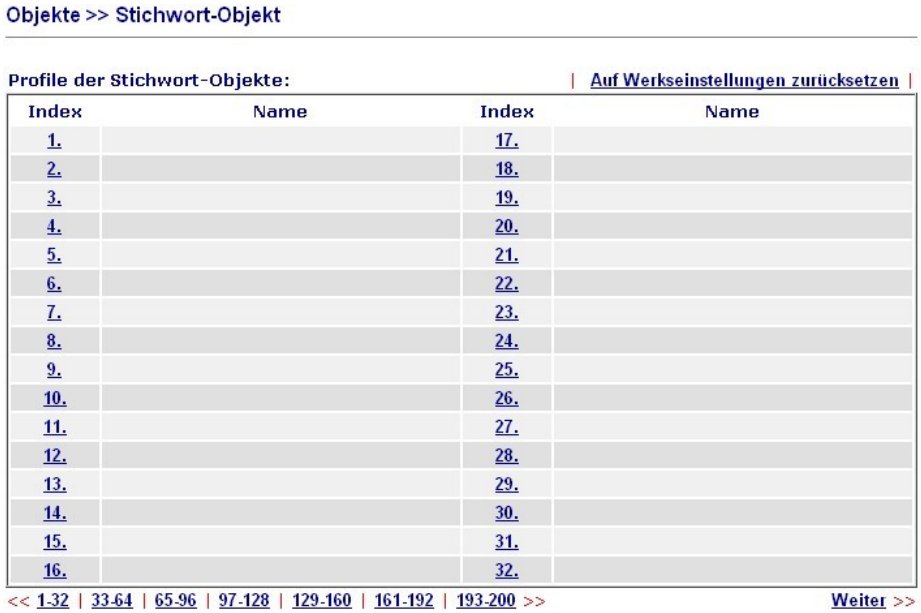
Name - Geben Sie für dieses Profil eine Bezeichnung ein.

Verfügbare Servicetyp-Objekte - Dieses Feld zeigt alle verfügbaren Servicetyp-Objekte an, die Sie unter **Objekte>>Servicetyp-Objekt** hinzugefügt haben.

Ausgewählte Servicetyp-Objekte - Klicken Sie auf die Taste >>, um die ausgewählten IP-Objekte in diesem Feld hinzuzufügen.

5.5.5 Stichwort-Objekt

Sie können bis zu 200 Stichwort-Objektprofile zur Auswahl als Blacklist oder Whitelist unter **CSM >>Inhaltsbezogener URL-Filter/Inhaltsbezogener Web-Filter** einrichten.



Auf Werkseinstellungen zurücksetzen Alle Profile löschen.

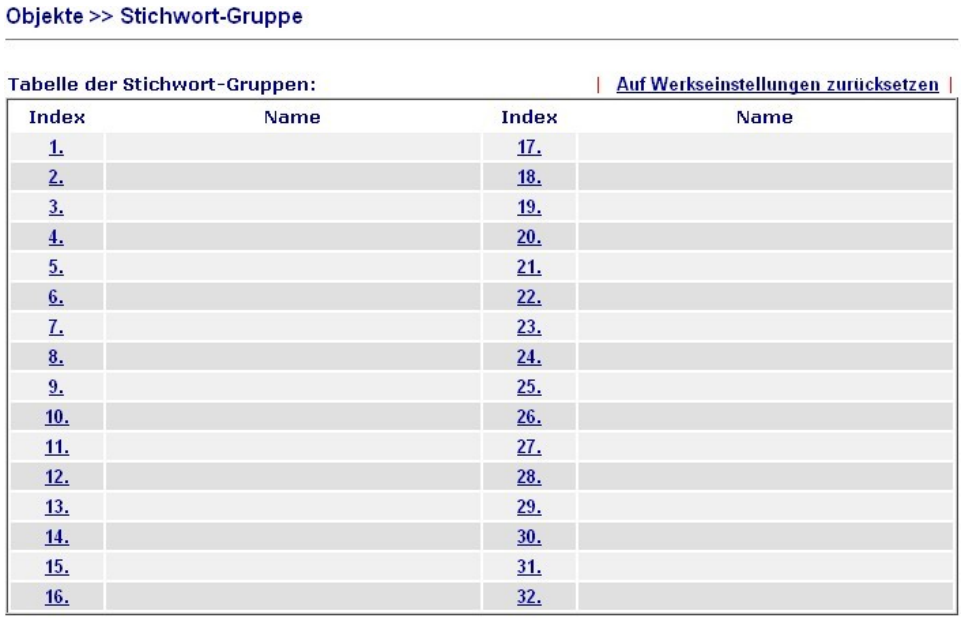
Klicken Sie auf die Nummer in der Indexspalte, um zu den Detaileinstellungen zu gelangen.

Name - Geben Sie für dieses Profil eine Bezeichnung ein, z.B. "Spiel".

Inhalt - Geben Sie den Inhalt des Profils ein, z.B. *Glücksspiel*. Beim Surfen im Internet wird dieser Begriff beobachtet und Seiten, welche diesen Begriff enthalten, gemäß den Firewall-Einstellungen entweder blockiert oder durchgelassen.

5.5.6 Stichwort-Gruppe

Diese Seite ermöglicht Ihnen, mehrere Stichwort-Objekte zu einer Gruppe zu verbinden. Die hier gesetzten Stichwort-Gruppen stehen unter **CSM >>Inhaltsbezogener URL-Filter/Inhaltsbezogener Web-Filter** zur Auswahl als Blacklist oder Whitelist.



Auf Werkseinstellungen zurücksetzen Alle Profile löschen.

Klicken Sie auf die Nummer in der Indexspalte, um zu den Detaileinstellungen zu gelangen.

Name - Geben Sie für diese Gruppe eine Bezeichnung ein.

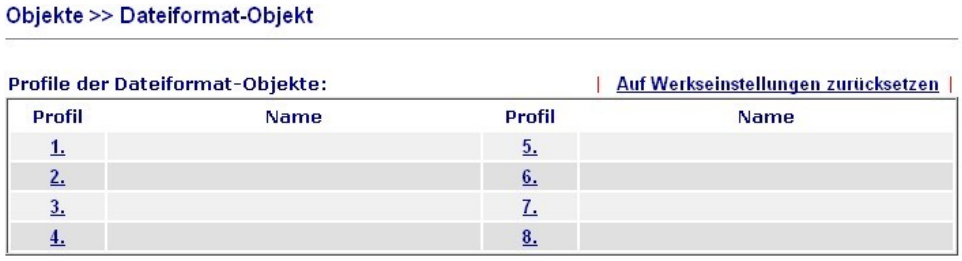
Verfügbare Stichwort-Objekte - Sie können Stichwort-Objekte von der Seite mit den Stichwort-Objekten zu einer Stichwort-Gruppe zusammenfassen. Sämtliche verfügbare Stichwort-Objekte, die Sie eingerichtet haben, werden in diesem Feld angezeigt.

Ausgewählte Stichwort-Objekte - Klicken Sie auf die Taste , um die ausgewählten Stichwort-Objekte in diesem Feld hinzuzufügen.

5.5.7 Dateiformat-Objekt

Auf dieser Seite können Sie bis zu acht Profile einrichten, die unter **CSM>>Inhaltsbezogener URL-Filter** zur Anwendung kommen. Alle Dateien mit den in diesen Profilen angegebenen Erweiterungen werden gemäß der gewählten Aktion verarbeitet.

Profil 1 mit der Bezeichnung "Standard" ist das Standardprofil. Die Dateien mit den in diesem Profil angegebenen Dateierweiterungen werden ignoriert und vom Vigor-Router nicht gescannt.



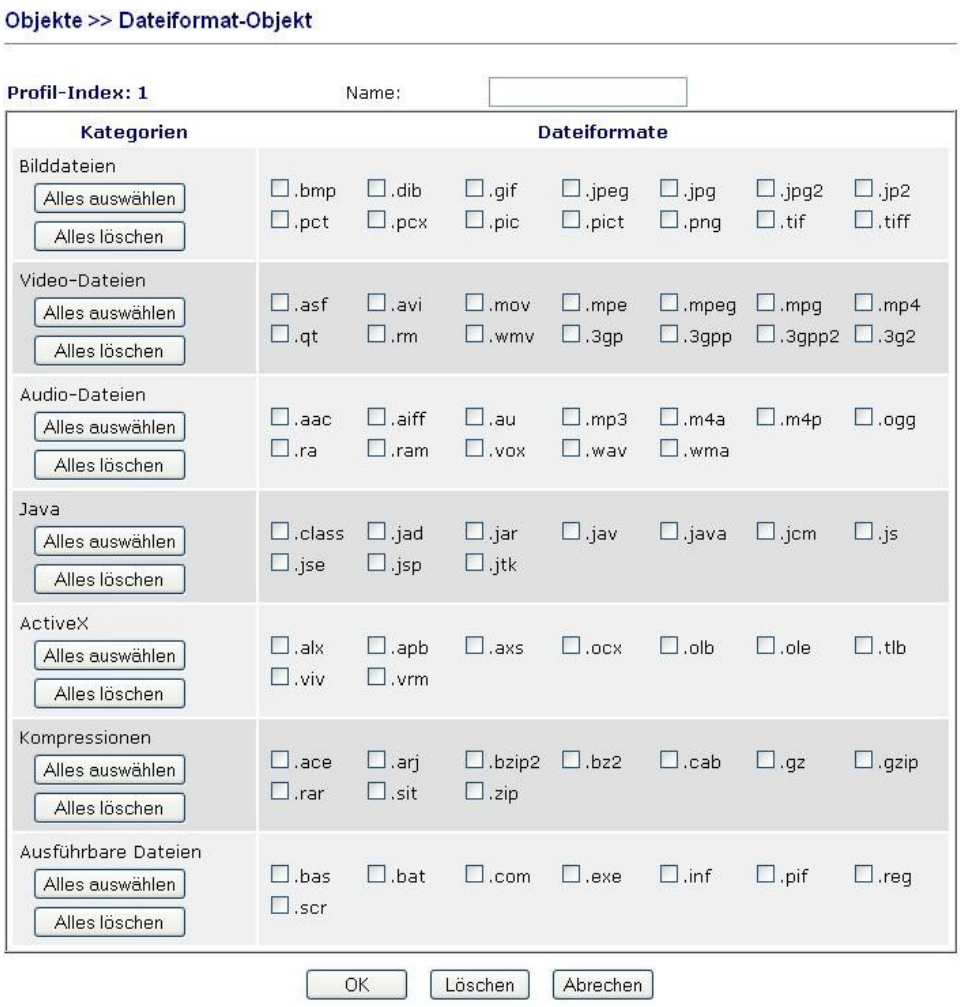
Auf Werkseinstellungen zurücksetzen Alle Profile löschen.

Klicken Sie für die Detailkonfiguration auf eine Nummer in der Profilspalte.

Profilname Geben Sie für dieses Profil einen Namen ein.

Geben Sie für das Profil eine Bezeichnung ein und markieren Sie alle

Dateierweiterungen, die von dem Router bearbeitet werden sollen. Klicken Sie abschließend auf **OK**, um das Profil zu speichern.



5.5.8 IM-Objekt

Auf dieser Seite können Sie bis zu 32 Profile für Instant Messenger einrichten. Diese Profile kommen unter **CSM>>IM-/P2P-Filter** als Filter zur Anwendung.

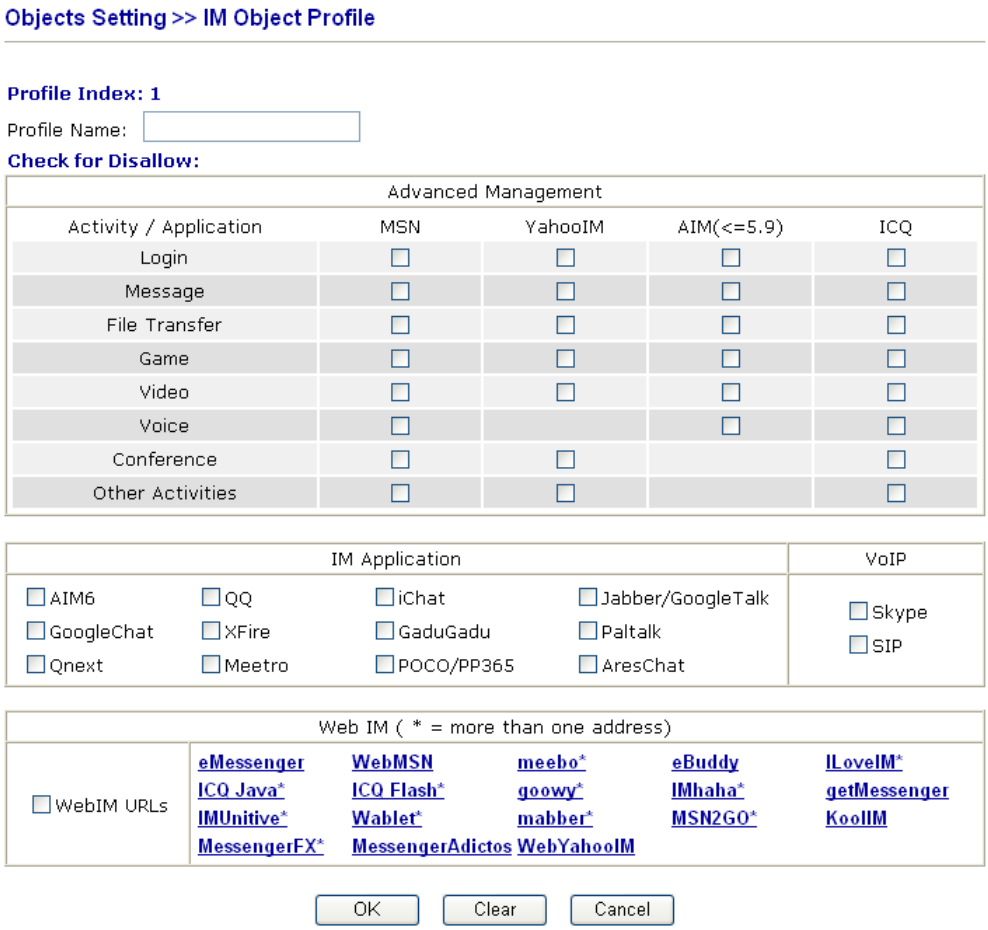
Objekte >> IM-Objekt

Profile der IM-Objekte: | Auf Werkseinstellungen zurücksetzen |

Profil	Name	Profil	Name
1.		17.	
2.		18.	
3.		19.	
4.		20.	
5.		21.	
6.		22.	
7.		23.	
8.		24.	
9.		25.	
10.		26.	
11.		27.	
12.		28.	
13.		29.	
14.		30.	
15.		31.	
16.		32.	

Auf Werkseinstellungen zurücksetzen Alle Profile löschen.

Klicken Sie für die Detailkonfiguration auf eine Nummer in der Profilspalte. Es werden verschiedene Instant Messenger (IM) aufgeführt, deren Benutzung Sie sperren können. Markieren Sie einfach die entsprechenden Kästchen und klicken auf **OK**. Auf der Seite **CSM>>IM-/P2P-Filter** können Sie die Dropdown-Liste **IM-Objekt** verwenden, um das richtige Profil als Standard für die Hosts zu wählen.

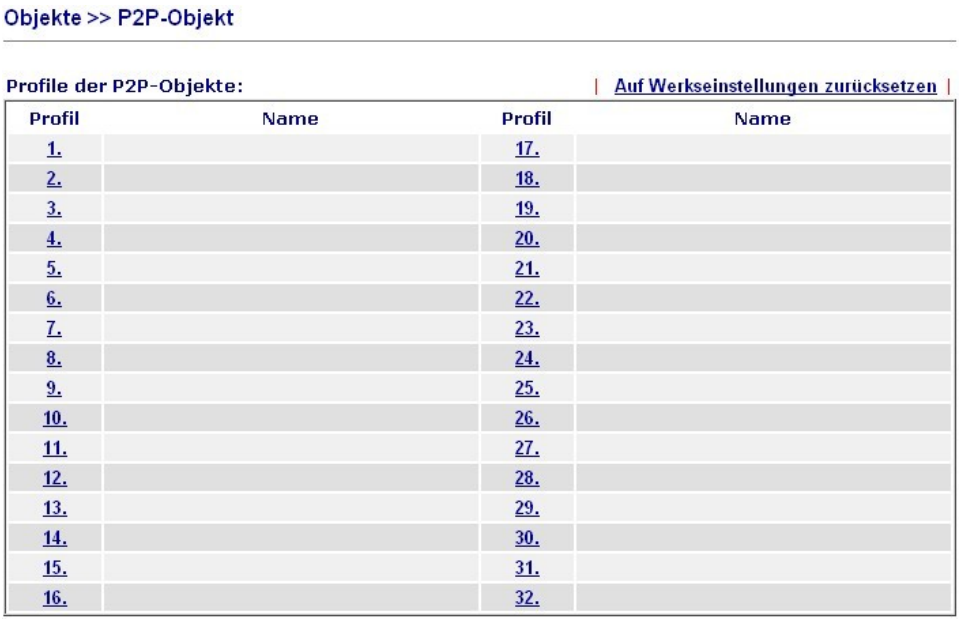


Profilname Geben Sie für dieses Profil einen Namen ein.

Geben Sie für das Profil eine Bezeichnung ein und markieren Sie sämtliche Punkte, die der Host nicht benutzen darf. Klicken Sie abschließend auf **OK**, um das Profil zu speichern.

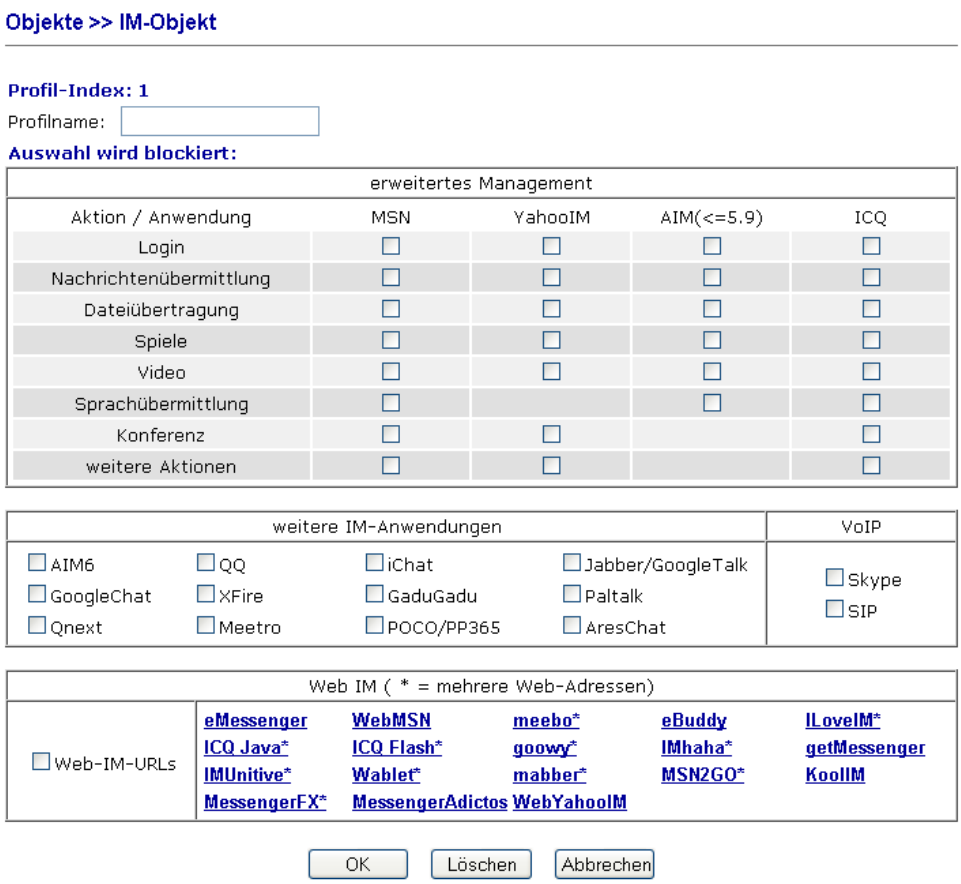
5.5.9 P2P-Objekt

Auf dieser Seite können Sie bis zu 32 Profile für P2P-Anwendungen einrichten. Diese Profile kommen unter **CSM>>IM-/P2P-Filter** als Filter zur Anwendung.



Auf Werkseinstellungen zurücksetzen Alle Profile löschen.

Klicken Sie für die Detailkonfiguration auf eine Nummer in der Profilspalte. Es werden verschiedene P2P-Protokolle aufgeführt, deren Benutzung Sie sperren können. Markieren Sie einfach die entsprechenden Kästchen und klicken auf **OK**. Auf der Seite **CSM>>IM-/P2P-Filter** können Sie später die Dropdown-Liste **P2P-Objekt** verwenden, um das richtige Profil als Standard für die folgenden Hosts zu wählen.

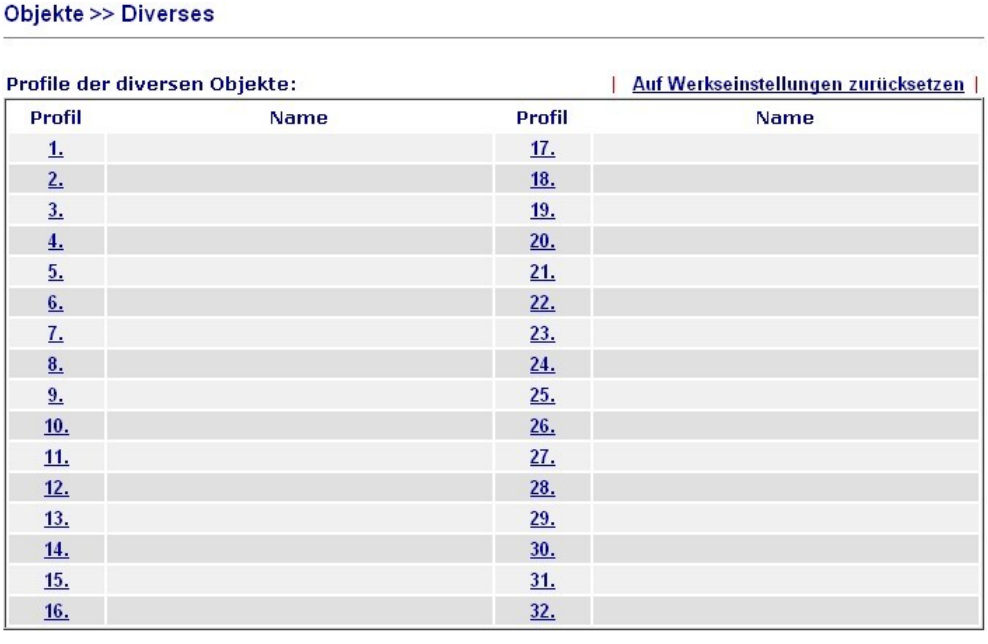


Profilname Geben Sie für dieses Profil einen Namen ein.

Geben Sie für das Profil eine Bezeichnung ein und markieren Sie sämtliche Protokolle, die der Host nicht benutzen darf. Klicken Sie abschließend auf **OK**, um das Profil zu speichern.

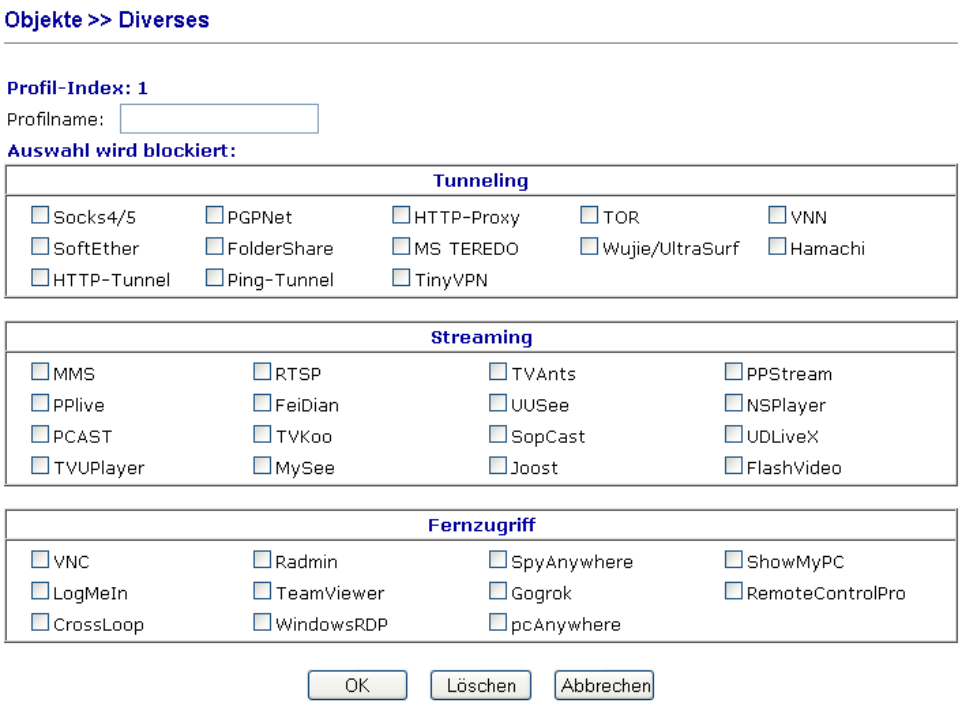
5.5.10 Diverses

Auf dieser Seite können Sie bis zu 32 Profile für verschiedene Anwendungen einrichten. Diese Profile kommen unter **CSM>>IM-/P2P-Filter** als Filter zur Anwendung.



Auf Werkseinstellungen zurücksetzen Alle Profile löschen.

Klicken Sie für die Detailkonfiguration auf eine Nummer in der Profilspalte. Auf der Seite werden Tunnel- und Streaming-Anwendungen aufgeführt, deren Benutzung Sie sperren können. Markieren Sie einfach die entsprechenden Kästchen und klicken auf **OK**. Auf der Seite **CSM>>IM-/P2P-Filter** können Sie später die Dropdown-Liste **Diverse Objekte** verwenden, um das entsprechende Profil als Standard für die folgenden Hosts zu wählen.



Profilname Geben Sie für dieses Profil einen Namen ein.

Geben Sie für das Profil eine Bezeichnung ein und markieren Sie sämtliche Protokolle, die der Host nicht benutzen darf. Klicken Sie abschließend auf **OK**, um das Profil zu speichern.

5.6 CSM

CSM ist die Abkürzung für **Content Security Management**, einer Funktion zur Steuerung der IM/P2P-Nutzung und Filterung von Web- und URL-Inhalten.

IM/P2P-Filter

Die Verbreitung verschiedener Instant Messenger Anwendungen hat die Kommunikation enorm vereinfacht. Während einige Unternehmen diese als nützliche Tools für Kundenkontakte fördern, befürchten andere Unternehmen jedoch den Missbrauch solcher Anwendungen während der Arbeitszeit oder unbekannte Sicherheitsrisiken. Die Situation ist bei P2P-Anwendungen ähnlich, da File Sharing zwar praktisch, aber auch unsicher sein kann. Die CSM-Funktionalität des Routers trägt diesen Anforderungen Rechnung.

Inhaltsbezogener URL-Filter

Um Benutzern eine geeignete Arbeitsumgebung zu schaffen, verfügt der Vigor-Router über einen **inhaltsbezogenen URL-Filter**, mit dem der unerwünschte Zugang von/zu unpassenden Web-Seiten vermieden wird und Web-Inhalte gesperrt werden, in denen sich bösartiger Code verbergen könnte.

Wenn ein Benutzer eine URL anklickt oder eingibt, die unerwünschte Stichwörter

enthält, wird der HTTP-Request für die jeweilige Web-Seite durch den URL-Stichwortfilter blockiert, so dass der Benutzer keinen Zugriff auf die Seite hat. Man könnte sich den **inhaltsbezogenen URL-Filter** als gewissenhaften Verkäufer vorstellen, der Teenagern keine Zeitschriften verkauft, die nicht jugendfrei sind. Im Büro sorgt der **inhaltsbezogene URL-Filter** dafür, dass nur auf betrieblich relevante Inhalte zugegriffen werden kann, um die Arbeitsleistung zu steigern. Ein inhaltsbezogener URL-Filter ist in Bezug auf die Filterung wirkungsvoller als eine konventionelle Firewall. Dies liegt daran, dass der Filter die URL-Zeichenfolgen und einige der HTTP-Daten, die sich im Nutzdatenteil der TCP-Pakete verbergen, überprüft, während traditionelle Firewalls Pakete lediglich anhand der Felder in TCP/IP-Headern überprüfen.

Außerdem kann der Vigor-Router Benutzer davon abhalten, aus Versehen schädlichen Code von Web-Seiten herunterzuladen. Schädlicher Code verbirgt sich oft in ausführbaren Objekten wie ActiveX, Java Applets, komprimierten Dateien und anderen ausführbaren Dateien. Das Herunterladen solcher Dateien von Web-Seiten kann eine Bedrohung für Ihr System darstellen. Ein ActiveX-Control-Objekt wird oft verwendet, um eine interaktive Web-Funktion zu ermöglichen. Schädlicher Code, der sich in diesem Objekt verbirgt, kann so auf das System des Benutzers gelangen.

Inhaltsbezogener Web-Filter

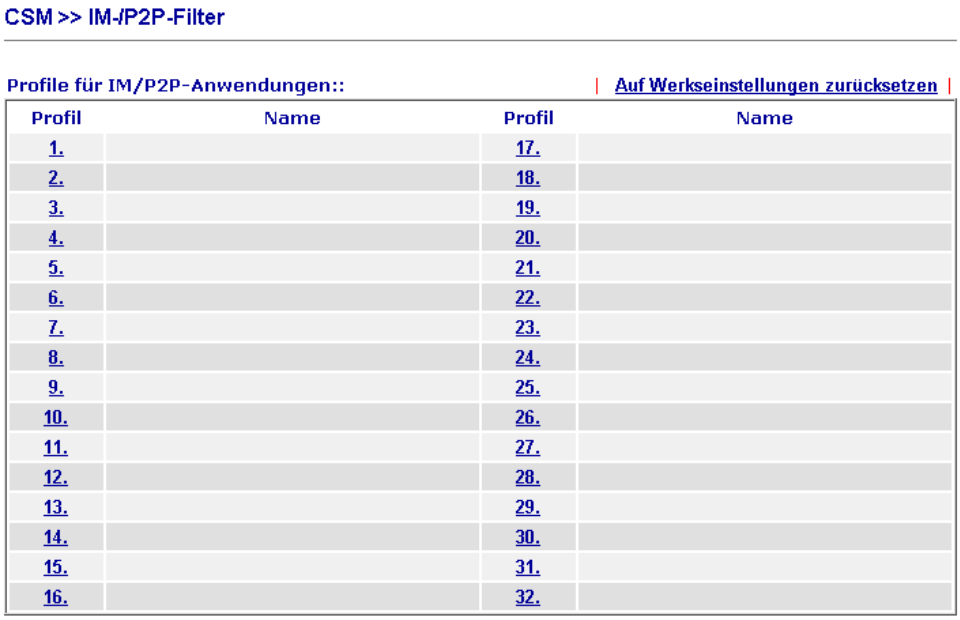
Wir alle sind uns bewusst, dass Internetinhalte bisweilen unangebracht sein können, wie dies auch bei anderen Medien der Fall sein kann. Als verantwortlicher Elternteil oder Arbeitgeber sollten Sie die Personen, die Ihnen anvertraut sind, vor Gefahren schützen. Mit dem Web-Filterdienst des Vigor-Routers können Sie Ihr Unternehmen vor üblichen direkten Gefahren schützen, welche Produktivität, gesetzliche Haftung, Netzwerk und Sicherheit bedrohen. Eltern können ihre Kinder vor dem Laden nicht jugendfreier Web-Seiten oder Chaträumen schützen.

Wenn Sie die Web-Filterfunktion des Vigor-Routers aktivieren und die Kategorien einrichten, die Sie einschränken möchten, wird jede angeforderte URL (z.B. www.bbc.co.uk) mit unserer Server-Datenbank abgeglichen. Diese Datenbank wird regelmäßig aktualisiert (dazu zählen natürlich auch lokale Angebote). Der Server fragt die URL ab und liefert Ihrem Router eine Kategorie. Ihr Vigor-Router entscheidet dann anhand der von Ihnen gewählten Kategorien, ob der Zugriff auf diese Seite erlaubt wird oder nicht. Da die Last auf verschiedene Datenbankserver verteilt wird, die Millionen von Kategorisierungsanfragen beantworten können, besteht kein Grund, durch diese Aktion eine Verzögerung beim Surfen zu befürchten.

Hinweis: Der inhaltsbezogene URL-Filter hat eine höhere Priorität als der inhaltsbezogene Web-Filter.

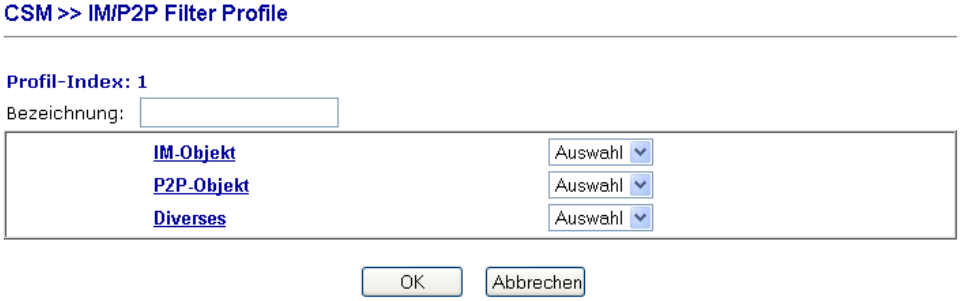
5.6.1 IM-/P2P-Filter

Sie können für verschiedene IM (Instant Messenger)/P2P (Peer to Peer) Anwendungen unterschiedliche Profile einrichten. Diese Profile werden unter **Firewall>>Basiskonfiguration** und **Firewall>>Filtereinstellung** verwendet.



Auf Werkseinstellungen zurücksetzen Alle Profile löschen.

Klicken Sie auf die Nummer in der Indexspalte, um zu den Detaileinstellungen zu gelangen.



Profilname Geben Sie einen Namen für das CSM-Profil ein.

Jedes Profil kann bis zu drei Objekteinstellungen enthalten: IM-Objekt, P2P-Objekt und diverses Objekt. Ein solches Profil kann unter **Firewall>>Basiskonfiguration** und **Firewall>>Filtereinstellung** als Standard für die folgenden Hosts bestimmt werden.

5.6.2 Inhaltsbezogener URL-Filter

Um Benutzern eine geeignete Arbeitsumgebung zu schaffen, verfügt der Vigor-Router über einen **inhaltsbezogenen URL-Filter**, mit dem der unerwünschte Zugang von/zu unpassenden Web-Seiten vermieden wird und Web-Inhalte gesperrt werden, in denen sich bösartiger Code verbergen könnte.

Wenn ein Benutzer eine URL anklickt oder eingibt, die unerwünschte Stichwörter enthält, wird der HTTP-Request für die jeweilige Web-Seite durch den URL-Stichwortfilter blockiert, so dass der Benutzer keinen Zugriff auf die Seite hat. Man könnte sich den **inhaltsbezogenen URL-Filter** als gewissenhaften Verkäufer vorstellen, der Teenagern keine Zeitschriften verkauft, die nicht jugendfrei sind. Im

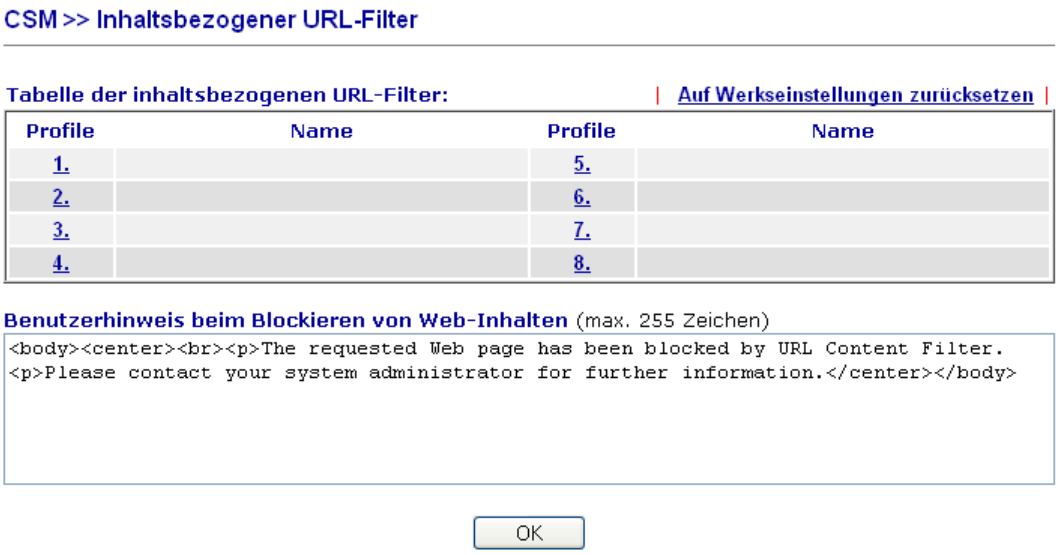
Büro sorgt der **inhaltsbezogene URL-Filter** dafür, dass nur auf betrieblich relevante Inhalte zugegriffen werden kann, um die Arbeitsleistung zu steigern. Ein inhaltsbezogener URL-Filter ist in Bezug auf die Filterung wirkungsvoller als eine konventionelle Firewall. Dies liegt daran, dass der Filter die URL-Zeichenfolgen und einige der HTTP-Daten, die sich im Nutzdatenteil der TCP-Pakete verbergen, überprüft, während traditionelle Firewalls Pakete lediglich anhand der Felder in TCP/IP-Headern überprüfen.

Außerdem kann der Vigor-Router Benutzer davon abhalten, aus Versehen schädlichen Code von Web-Seiten herunterzuladen. Schädlicher Code verbirgt sich oft in ausführbaren Objekten wie ActiveX, Java Applets, komprimierten Dateien und anderen ausführbaren Dateien. Das Herunterladen solcher Dateien von Web-Seiten kann eine Bedrohung für Ihr System darstellen. Ein ActiveX-Control-Objekt wird oft verwendet, um eine interaktive Web-Funktion zu ermöglichen. Schädlicher Code, der sich in diesem Objekt verbirgt, kann so auf das System des Benutzers gelangen.

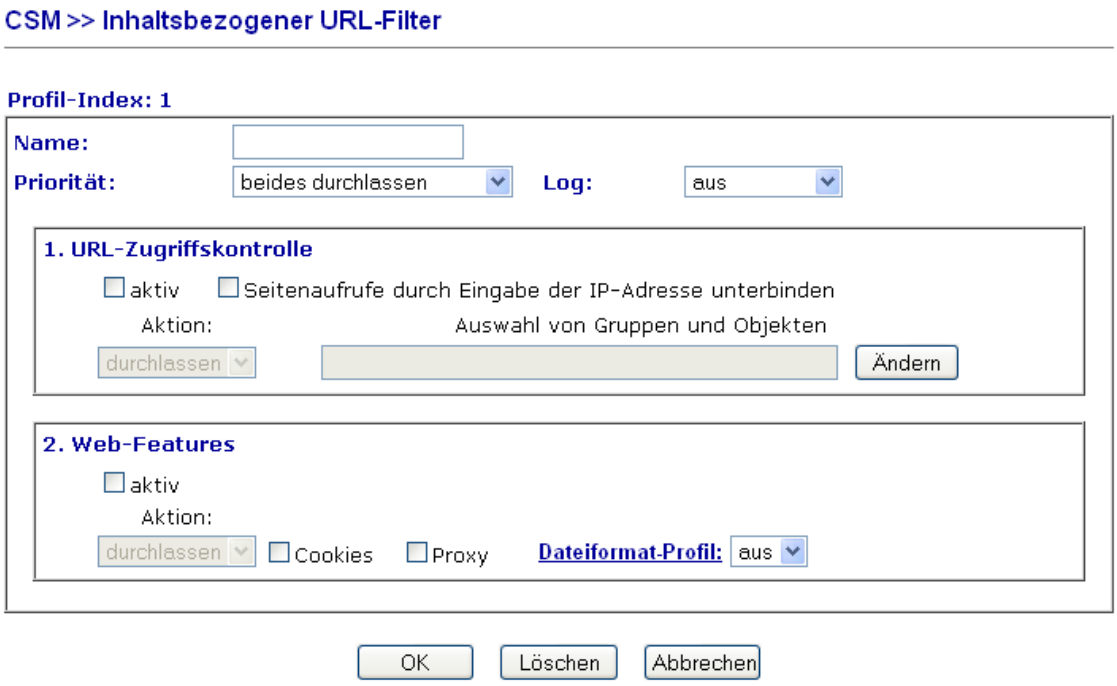
Falls Sie beispielsweise Wörter wie "Sex" hinzufügen, blockiert der Vigor-Router den Zugriff auf Web-Sites oder Web-Seiten wie "www.sex.com" oder www.backdoor.net/images/sex/p_386.html. Sie können auch einfach die gesamte URL (z.B. "www.sex.com") oder einen Teil davon (z.B. "sex.com") angeben.

Der Vigor-Router wird jegliche Anforderungen verwerfen, die versuchen, schädlichen Code abzurufen.

Klicken Sie auf **CSM** und wählen Sie **Inhaltsbezogener URL-Filter**, um die Konfigurationsseite für das Profil zu öffnen.



Sie können bis zu acht Profile als inhaltsbezogene URL-Filter setzen. Klicken Sie einfach die Indexnummer unter Profil an, um den folgenden Dialog zu öffnen.



Profilname - Geben Sie den Profilnamen ein.

Priorität - Bestimmt die Aktion, die der Router durchführen wird.

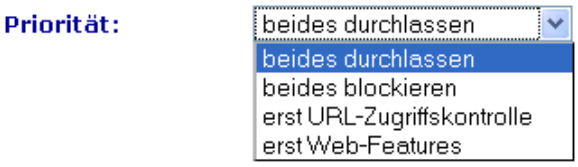
Beides durchlassen – Der Router lässt alle Pakete durch, die den unter URL-Zugriffskontrolle und Web-Features unten angegebenen Bedingungen entsprechen. Falls Sie diese Einstellung wählen, werden die Konfigurationen für die URL-Zugriffskontrolle und Web-Features auf dieser Seite deaktiviert.

Beides blockieren – Der Router blockiert alle Pakete, die den unter URL-Zugriffskontrolle und Web-Features unten angegebenen Bedingungen entsprechen. Falls Sie diese Einstellung wählen, werden die Konfigurationen für die URL-Zugriffskontrolle und Web-Features auf dieser Seite deaktiviert.

Erst URL-Zugriffskontrolle – Falls alle Pakete den Bedingungen entsprechen, die unter URL-Zugriffskontrolle und Web-Features unten angegeben sind, kann dies die Priorität der ausgeführten Aktion bestimmen. Bei dieser Option verarbeitet der Router die Pakete zunächst mit den Bedingungen für URLs und dann mit den Bedingungen für Web-Features wie unten angegeben.

Erst Web-Features – Falls alle Pakete den Bedingungen entsprechen, die unter URL-Zugriffskontrolle und Web-Features unten angegeben sind, kann dies die Priorität der ausgeführten Aktion bestimmen. Bei dieser Option verarbeitet der Router die Pakete zunächst mit den Bedingungen für Web-

Features und dann mit den Bedingungen für URLs wie unten angegeben.



LogKeine – Für dieses Profil wird keine Log-Datei aufgezeichnet.

Durchlassen – Lediglich Meldungen zum Durchlassen werden im Syslog aufgezeichnet.

Blockieren – Lediglich Meldungen zum Blockieren werden im Syslog aufgezeichnet.

Alle – Alle Aktionen (Durchlassen und Blockieren) werden im Syslog aufgezeichnet.

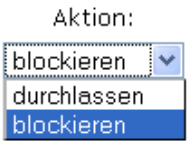
URL-ZugriffskontrolleAktiv - Markieren Sie dieses Kästchen, um die URL-Zugriffskontrolle zu aktivieren. Beachten Sie, dass die Priorität der **URL-Zugriffskontrolle** höher ist als die der **Web-Features**. Falls der Web-Inhalt den Einstellungen der URL-Zugriffskontrolle entspricht, führt der Router die in diesem Feld angegebene Aktion aus und ignoriert die unter Web-Features angegebene Aktion.

Seitenaufrufe durch Eingabe der IP-Adresse unterbinden - Markieren Sie dieses Kästchen, um Surfen durch Eingabe der IP-Adresse (z.B. http://202.6.5.2) zu unterbinden. Dadurch kann vermieden werden, dass jemand die URL-Zugriffskontrolle umgeht. Sie müssen Ihren Browser-Cache zunächst löschen, damit die inhaltsbezogene URL-Filterfunktion auf zuvor besuchten Web-Seiten ordnungsgemäß funktioniert.

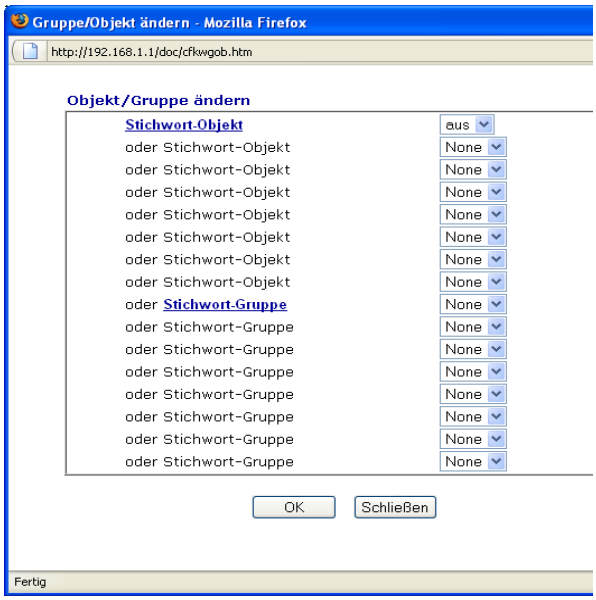
Aktion – Diese Einstellung ist nur verfügbar, falls entweder **Erst URL-Zugriffskontrolle** oder **Erst Web-Features** gewählt wurde. ***Durchlassen*** - Zugriff auf die entsprechende Web-Seite mit den im Feld unten aufgeführten Stichwörtern zulassen.

Blockieren **-** Zugriff auf die entsprechende Web-Seite mit den im Feld unten aufgeführten Stichwörtern blockieren.

Falls die Web-Seiten nicht den hier angegebenen Stichwörtern entsprechen, werden sie mit der entgegengesetzten Aktion verarbeitet.



Auswahl von Gruppen und Objekten – Der Vigor-Router ermöglicht Benutzern die Definition von Stichwörtern, wobei jedes Frame die Angabe von mehreren Stichwörtern erlaubt. Das Stichwort kann ein Nomen, ein Teil davon oder eine komplette URL sein. Mehrere Stichwörter innerhalb eines Frames werden durch Leerzeichen, Komma oder Semikolon getrennt. Die maximale Länge jedes Frames beträgt 32 Zeichen. Nach Angabe von Stichwörtern wird der Vigor-Router Verbindungen zur Web-Site ablehnen, deren URL-Zeichenfolge irgendeinem benutzerdefinierten Stichwort entspricht. Je einfacher die Liste der zu blockierenden Stichwörter ist, desto effizienter wird der Vigor-Router arbeiten.



Web-FeaturesAktiv - Markieren Sie dieses Kästchen, damit das Stichwort blockiert bzw. durchgelassen wird.

Aktion – Diese Einstellung ist nur verfügbar, falls entweder **Erst URL-Zugriffskontrolle** oder **Erst Web-Features** gewählt wurde. **Durchlassen** erlaubt den Zugriff auf die entsprechende Web-Seite mit den im Feld unten aufgeführten Stichwörtern.

***Durchlassen* -** Zugriff auf die entsprechende Web-Seite mit den im Feld unten aufgeführten Stichwörtern zulassen.

***Blockieren* -** Zugriff auf die entsprechende Web-Seite mit den im Feld unten aufgeführten Stichwörtern blockieren.

Falls die Web-Seiten nicht den hier angegebenen Features entsprechen, werden sie mit der entgegengesetzten Aktion verarbeitet.

Cookies - Markieren Sie dieses Kästchen, um die Übertragung von Cookies zu unterbinden, um die Privatsphäre des lokalen Benutzers zu schützen.

Proxy - Markieren Sie dieses Kästchen, um jegliche Proxy-Übertragung abzulehnen. Um die begrenzte Bandbreitennutzung wirksam zu steuern, ist es sinnvoll, den Blockiermechanismus zu aktivieren, welcher die von Web-Seiten heruntergeladenen Dateien ausfiltert.

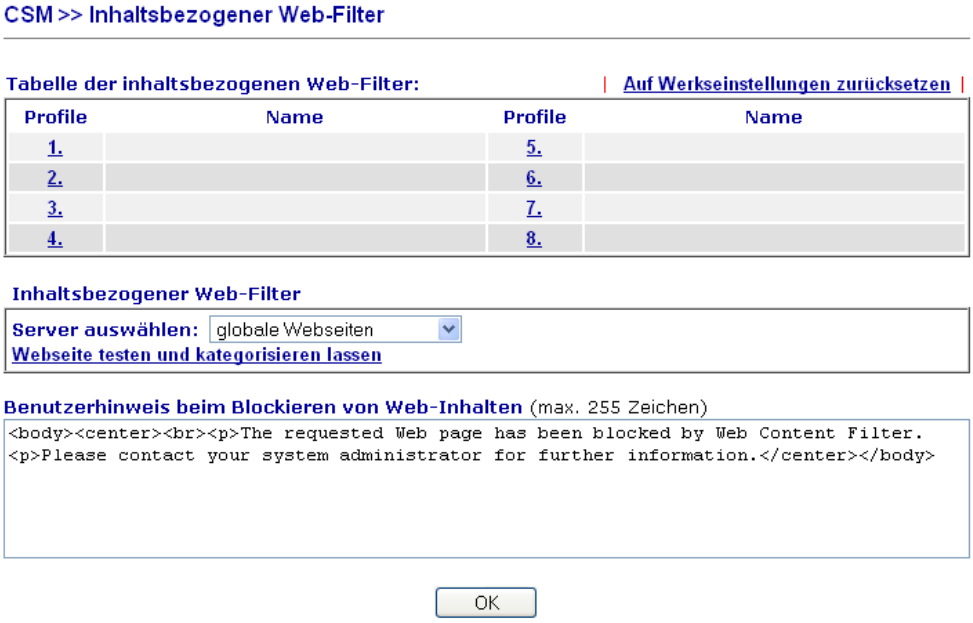
Dateiformat-Profil – Wählen Sie eines der Profile, das Sie bereits unter **Objekte>> Dateiformat-Objekt** zum Durchlassen oder Blockieren von Datei-Downloads eingerichtet haben.

5.6.3 Inhaltsbezogener Web-Filter

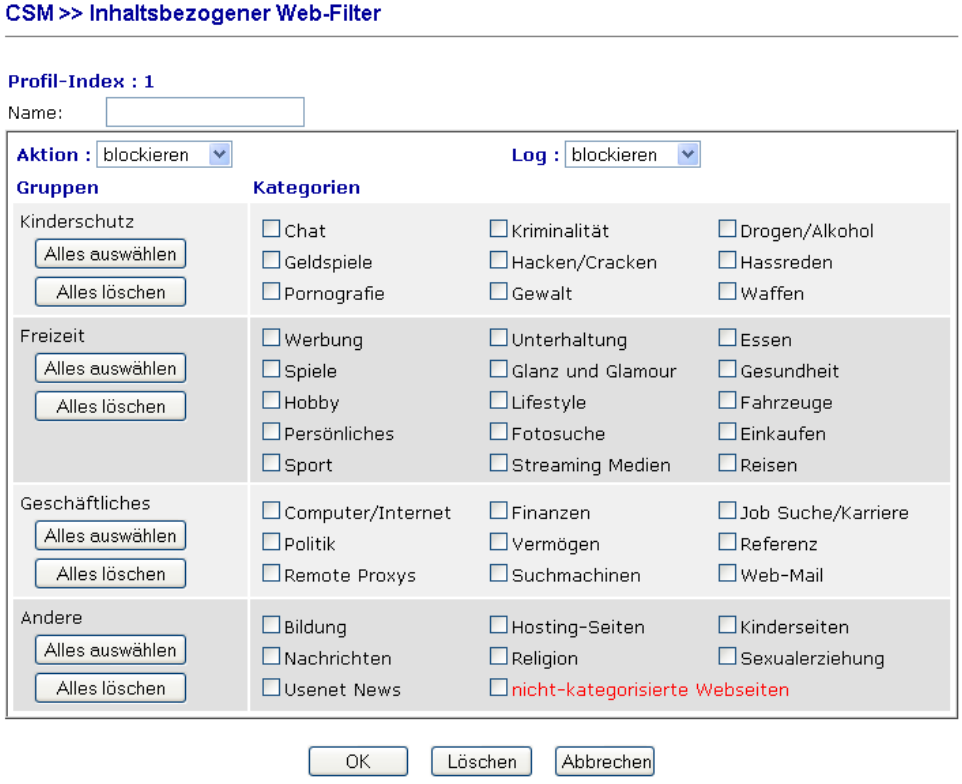
Wir alle sind uns bewusst, dass Internetinhalte bisweilen unangebracht sein können, wie dies auch bei anderen Medien der Fall sein kann. Als verantwortlicher Elternteil oder Arbeitgeber sollten Sie die Personen, die Ihnen anvertraut sind, vor Gefahren schützen. Mit dem Web-Filterdienst des Vigor-Routers können Sie Ihr Unternehmen vor üblichen direkten Gefahren schützen, welche Produktivität, gesetzliche Haftung, Netzwerk und Sicherheit bedrohen. Eltern können ihre Kinder vor dem Laden nicht jugendfreier Web-Seiten oder Chaträumen schützen.

Wenn Sie die Web-Filterfunktion des Vigor-Routers aktivieren und die Kategorien einrichten, die Sie einschränken möchten, wird jede angeforderte URL (z.B. www.bbc.co.uk) mit unserer Server-Datenbank abgeglichen. Diese Datenbank wird regelmäßig aktualisiert (dazu zählen natürlich auch lokale Angebote). Der Server fragt die URL ab und liefert Ihrem Router eine Kategorie. Ihr Vigor-Router entscheidet dann anhand der von Ihnen gewählten Kategorien, ob der Zugriff auf diese Seite erlaubt wird oder nicht. Da die Last auf verschiedene Datenbankserver verteilt wird, die Millionen von Kategorisierungsanfragen beantworten können, ist die Verzögerung beim Surfen minimal.

Klicken Sie auf **CSM** und wählen Sie **Inhaltsbezogener Web-Filter**, um die Konfigurationsseite für das Profil zu öffnen.



Sie können bis zu acht Profile als inhaltsbezogene Web-Filter setzen. Klicken Sie einfach die Indexnummer unter Profil an, um den folgenden Dialog zu öffnen.



AktionDurchlassen - Zugriff auf die entsprechende Web-Seite mit den im Feld unten aufgeführten Kategorien zulassen.

Blockieren - Zugriff auf die entsprechende Web-Seite mit den im Feld unten aufgeführten Kategorien blockieren.

Falls die Web-Seiten nicht den hier angegebenen Features entsprechen, werden sie mit der entgegengesetzten Aktion verarbeitet.

LogKeine – Für dieses Profil wird keine

Log-Datei aufgezeichnet.

Durchlassen – Lediglich Meldungen zum Durchlassen werden im Syslog aufgezeichnet.

Blockieren – Lediglich Meldungen zum Blockieren werden im Syslog aufgezeichnet.

Alle – Alle Aktionen (Durchlassen und Blockieren) werden im Syslog aufgezeichnet.

Sehen Sie hierzu auch die Benutzerinformation zum **Inhaltsbezogenen Web-Filter**.

5.7 Bandbreitenmanagement

Die folgende Abbildung zeigt die Menüeinträge für das Bandbreitenmanagement:

5.7.1 Sitzungen begrenzen

Ein PC mit einer privaten IP-Adresse kann über den NAT-Router auf das Internet zugreifen. Der Router erzeugt für eine solche Verbindung die Einträge der NAT-Sitzung. P2P (Peer to Peer) Anwendungen (z.B. BitTorrent) benötigen immer viele Sitzungen für den Betrieb und belegen oft so viele Ressourcen, dass wichtige Zugriffe behindert werden. Um dieses Problem zu lösen, können Sie die Anzahl der Sitzungen für die angegebenen Hosts beschränken.

Klicken Sie im Menü **Bandbreitenmanagement** auf **Sitzungen begrenzen**, um den entsprechenden Dialog zu öffnen.

Um die Funktion zur Begrenzung von Sitzungen zu aktivieren, klicken Sie einfach auf **Aktiv** und geben die Standardgrenze für Sitzungen ein.

Aktiv - Klicken Sie auf diese Taste, um die Sitzungsbegrenzungsfunktion zu aktivieren.

Inaktiv - Klicken Sie auf diese Taste, um die Sitzungsbegrenzungsfunktion zu deaktivieren.

Standard Sitzungslimit - Legt die standardmäßige Anzahl der Sitzungen für jeden Rechner im LAN fest.

Begrenzungsliste - Zeigt eine Liste spezifischer Begrenzungen an, die Sie in diesem Dialog eingerichtet haben.

Start-IP - Bestimmt die Start-IP-Adresse für die Sitzungsbegrenzung.

End-IP - Bestimmt die End-IP-Adresse für die Sitzungsbegrenzung.

Maximale Sitzungen - Gibt die verfügbare Anzahl der Sitzungen für jeden Host im angegebenen IP-Adressbereich an. Falls Sie in diesem Feld keine Anzahl von Sitzungen angeben, verwendet das System das Standard-Sitzungslimit für die von Ihnen für jeden Index gesetzte spezifische Begrenzung.

Hinzufügen - Fügt der obigen Liste die spezifische Sitzungsbegrenzung hinzu.

Bearbeiten - Ermöglicht Ihnen, die Einstellungen der gewählten Begrenzung zu bearbeiten.

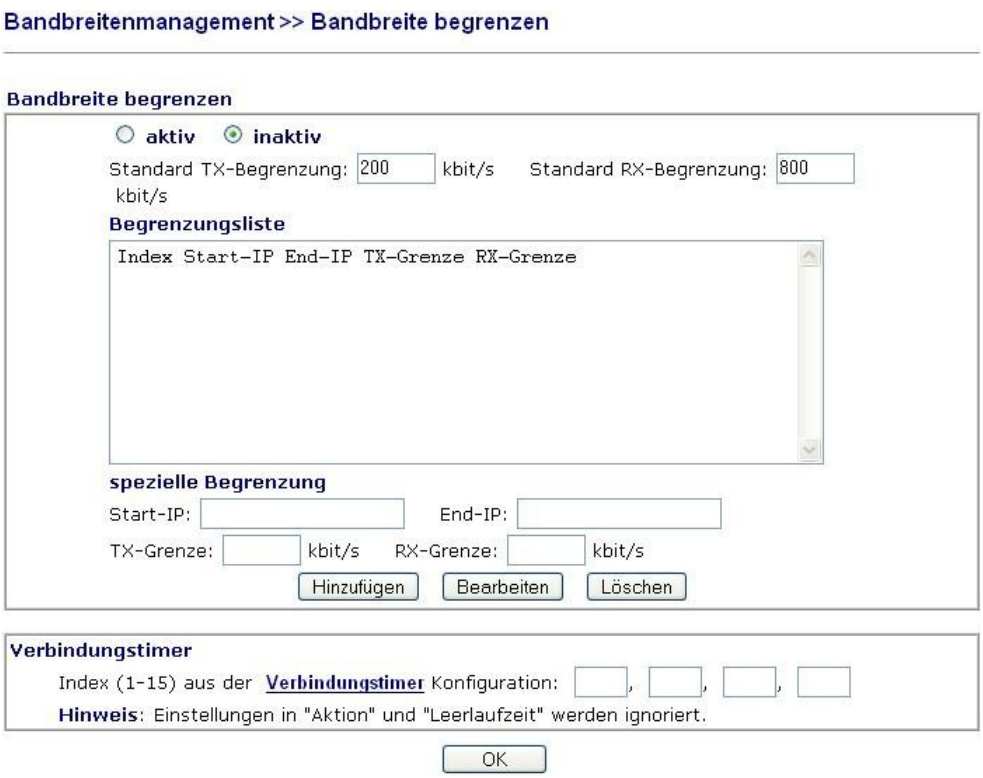
Entfernen - Gewählte Einstellungen von der Begrenzungsliste entfernen.

Index (1-15) aus der Verbindungstimer Konfiguration - Sie können für Ihre Anforderungen vier Verbindungstimer einrichten. Alle Verbindungstimer können im Voraus im Dialog **Anwendungen – Verbindungstimer** eingestellt werden, und Sie können die Nummer verwenden, die Sie in jenem Dialog gesetzt haben.

5.7.2 Bandbreitenbegrenzung

Der Downstream- und Upstream-Datenfluss von FTP-, HTTP- und einigen P2P-Anwendungen kann viel Bandbreite in Anspruch nehmen und somit andere Anwendungen beeinträchtigen. Sie können die Bandbreitenbegrenzung einsetzen, um die Bandbreite effizienter zu nutzen.

Klicken Sie im Menü **Bandbreitenmanagement** auf **Bandbreite begrenzen**, um den entsprechenden Dialog zu öffnen.



Um die Funktion zur Bandbreitenbegrenzung zu aktivieren, klicken Sie einfach auf **Aktiv** und geben die Standardgrenzen für Upstream und Downstream ein.

Aktiv - Klicken Sie auf diese Taste, um die Bandbreitenbegrenzungsfunktion zu aktivieren.

Inaktiv - Klicken Sie auf diese Taste, um die Bandbreitenbegrenzungsfunktion zu deaktivieren.

Standard TX-Begrenzung - Definieren Sie die Standard-Upstream-Geschwindigkeit für jeden Rechner im LAN.

Standard RX-Begrenzung - Definieren Sie die Standard-Downstream-Geschwindigkeit für jeden Rechner im LAN.

Begrenzungsliste - Zeigt eine Liste spezifischer Begrenzungen an, die Sie in diesem Dialog eingerichtet haben.

Start-IP - Geben Sie die Start-IP für die Begrenzung der Bandbreite ein.

End-IP - Geben Sie die End-IP für die Begrenzung der Bandbreite ein.

Max. TX - Bestimmen Sie die Begrenzung für die Upstream-Geschwindigkeit. Falls Sie in diesem Feld keine Grenze angeben, verwendet das System die Standardgeschwindigkeit für die von Ihnen für jeden Index gesetzte spezifische Begrenzung.

Max. RX - Bestimmen Sie die Begrenzung

für die Downstream-Geschwindigkeit. Falls Sie in diesem Feld keine Grenze angeben, verwendet das System die Standardgeschwindigkeit für die von Ihnen für jeden Index gesetzte spezifische Begrenzung.

Hinzufügen - Die spezifische Geschwindigkeitsbegrenzung der obigen Liste hinzufügen.

Bearbeiten - Ermöglicht Ihnen, die Einstellungen der gewählten Begrenzung zu bearbeiten.

Löschen - Gewählte Einstellungen von der Begrenzungsliste entfernen.

Index (1-15) aus dem Verbindungstimer Konfiguration - Sie können für Ihre Anforderungen vier Verbindungstimer einrichten. Alle Verbindungstimer können im Voraus im Dialog **Anwendungen – Verbindungstimer** eingestellt werden, und Sie können die Nummer verwenden, die Sie in jenem Dialog gesetzt haben.

5.7.3 QoS

Der Einsatz von QoS (Quality of Service) sorgt dafür, dass alle Anwendungen die erforderliche Dienstgüte und genügend Bandbreite erhalten, um die erwartete Leistung zu erbringen, was zweifellos ein wichtiger Aspekt eines modernen Unternehmensnetzwerks ist.

Ein Grund für den Einsatz von QoS ist, dass viele TCP-basierte Anwendungen ihre Übertragungsgeschwindigkeit im Verlauf der Sitzung erhöhen und dann möglicherweise die gesamte verfügbare Bandbreite in Anspruch nehmen (TCP Slow Start). Ohne QoS-Schutz würde ein großer Teil der Leistung anderer Anwendungen im übervollen Netzwerk verloren gehen. Dies ist besonders für Anwendungen wichtig, die gegenüber Verlusten, Verzögerungen oder Jitter (Laufzeitvarianz) empfindlich sind.

Ein anderer Grund für den Einsatz von QoS liegt in den Engpässen, die an Netzwerkkreuzungen entstehen können, an denen Netzwerkstrecken mit unterschiedlichen Geschwindigkeiten aufeinander treffen oder an denen sich der Verkehr staut und Pakete warten müssen, wodurch der Verkehr auf eine niedrigere Geschwindigkeit gedrosselt werden kann. Falls es keine definierte Priorität gibt, die bestimmt, welche Pakete aus einer überfließenden Warteschlange verworfen werden sollen, könnten Pakete empfindlicher Anwendungen betroffen sein. Wie wirkt sich dies auf die Anwendungsleistung aus?

Die primäre QoS-Konfiguration beinhaltet zwei Komponenten:

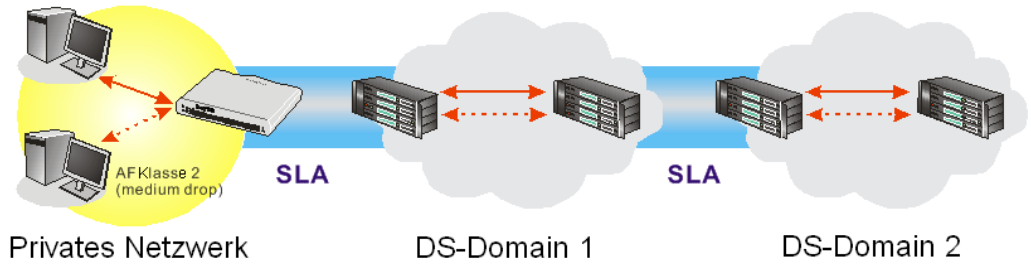
- Klassifizierung: Erkennung von kritischen Anwendungen und Anwendungen mit niedriger Latenz und Kennzeichnung für Dienstgüte mit hoher Priorität im gesamten Netzwerk.
- Zeitplanung: Zuweisung von Paketen zu Warteschlangen und Servicetypen auf der Grundlage der Klassifizierung der Dienstgüte.

Der grundlegende QoS-Ansatz der Vigor-Router besteht darin, Pakete aufgrund der Servicetyp-Information im IP-Header zu klassifizieren und einzuplanen. Um zum Beispiel die Verbindung zur Firmenzentrale zu sichern, kann ein Teleworker einen

QoS-Kontrollindex bestimmen, um Bandbreite für eine HTTPS-Verbindung zu sichern und gleichzeitig viele andere Anwendungen zu nutzen.

Ein weiterführender Ansatz des QoS-Netzwerk besteht in der Anwendung von DSCP (Differentiated Service Code Point) und IP Precedence Disziplinen auf Layer 3. Im Gegensatz zum herkömmlichen IP Precedence, welches das ToS (Type of Service) Feld im IP-Header verwendet, um acht Dienstklassen zu definieren, ermöglicht der Nachfolger DSCP 64 Klassen, wobei diese Technik mit IP Precendence abwärtskompatibel ist. In einem QoS-aktivierten Netzwerk oder Differentiated Service (DiffServ oder DS) System sollte der Inhaber der DS-Domain eine Dienstgütevereinbarung (SLA - Service Level Agreement) mit anderen DS-Domaininhabern unterzeichnen, um die Dienstgüte zu definieren, die für den Verkehr von verschiedenen Domains bereitgestellt wird. Dadurch wird jeder DS-Knoten in diesen Domains entsprechend priorisiert. Dies wird als Per-Hop Behavior (PHB) bezeichnet. Die Definition von PHB umfasst Expedited Forwarding (EF), Assured Forwarding (AF) und Best Effort (BE). AF bietet vier Lieferklassen (bzw. Weiterleitungsklassen) und drei Drop-Prioritätsstufen in jeder Klasse.

Als Edge-Router der DS-Domain überprüfen Vigor-Router den markierten DSCP-Wert im IP-Header des passierenden Verkehrs, um der Klassifizierung und Zeitplanung entsprechend Ressourcen zuzuweisen. Die Core-Router im Backbone wenden vor Ausführung die gleiche Überprüfung an, um im gesamten QoS-aktivierten Netzwerk die entsprechende Dienstgüte zu gewährleisten.



Jeder Knoten kann jedoch aufgrund der SLAs zwischen verschiedenen DS-Domaininhabern eine unterschiedliche Betrachtungsweise der Pakete mit hoher Priorität aufweisen. Es ist daher nicht einfach, alleine durch die Bemühungen des Vigor-Routers im gesamten Netzwerk konsequent QoS-Verkehr mit hoher Priorität zu ermöglichen.

Klicken Sie im Menü **Bandbreitenmanagement** auf **QoS**, um den entsprechenden Dialog zu öffnen.

Bandbreitenmanagement >> Quality of Service

Basiskonfiguration | Auf Werkseinstellungen zurücksetzen |

Index	Status	Bandbreite	Richtung	Gruppe 1	Gruppe 2	Gruppe 3	Andere	UDP-Bandbreiten Begrenzung	
WAN1	aktiv	--kbit/s /--kbit/s	Beide	25%	25%	25%	25%	aktiv	Bearbeiten
WAN2	aktiv	10000kbit/s /10000kbit/s	Raus	25%	25%	25%	25%	inaktiv	Bearbeiten

Gruppenregeln

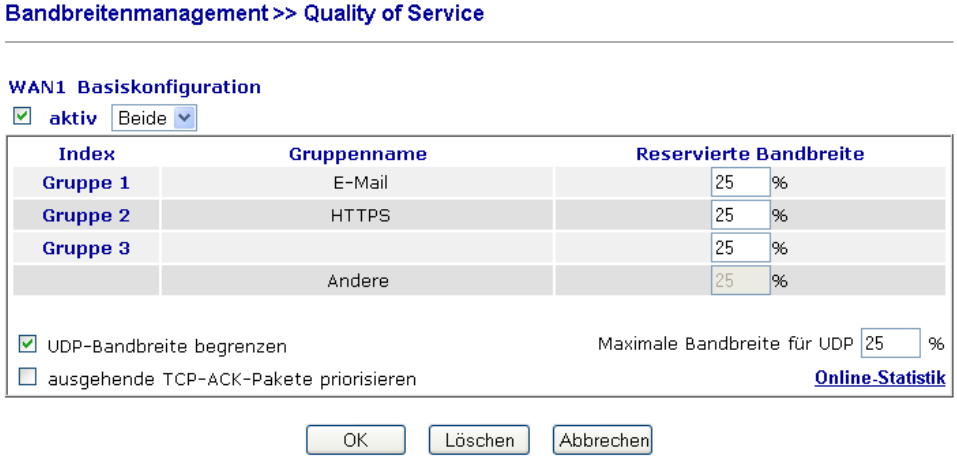
Index	Name	Regel	Servicetyp
Gruppe 1	E-Mail	Ändern	
Gruppe 2	HTTPS	Ändern	Ändern
Gruppe 3		Ändern	

Diese Seite zeigt QoS-Einstellungen der WAN-Schnittstelle an. Klicken Sie auf **Setup**, um für die Basiskonfiguration der WAN (1/2)-Schnittstelle auf die nächste Seite zu gelangen. Zur Konfiguration der Klassenregeln klicken Sie auf **Bearbeiten**.

Sie können die Basiskonfiguration der WAN-Schnittstelle, die Klassenregeln und den Servicetyp für die Klassenregeln Ihren Anforderungen entsprechend einrichten.

Basiskonfiguration der WAN-Schnittstelle

Klicken Sie auf **Konfiguration**, um die Bandbreite für QoS der WAN-Schnittstelle zu konfigurieren. Es sind vier Warteschlangen für die QoS-Kontrolle verfügbar. Die ersten drei Klassenregeln (Klasse 1 bis Klasse 3) können Ihren Anforderungen angepasst werden. Die letzte ist für die Pakete reserviert, die nicht für die benutzerdefinierten Klassenregeln geeignet sind.



Aktiv - Die Werkseinstellung wird aktiviert.

Bitte geben Sie auch an, auf welchen Verkehr die QoS-Einstellungen anzuwenden sind.

Rein - Nur auf eingehenden Verkehr anwenden.

Raus - Nur auf ausgehenden Verkehr anwenden.

Beide - Auf eingehenden und ausgehenden Verkehr anwenden.

Markieren Sie das Kästchen und klicken auf **OK**. Dann klicken Sie erneut auf **Konfiguration**. Der Link für **Online-Statistik** erscheint auf dieser Seite.

WAN-Bandbreite Inbound (rein) - Hier können Sie die Verbindungsgeschwindigkeit des WANs für eingehende Daten einstellen. Wenn Ihr ADSL beispielsweise 1 Mbit/s Downstream und 256 kbit/s Upstream unterstützt, geben Sie bitte in diesem Feld 1.000 kbit/s ein. Der Standardwert beträgt 1.000 kbit/s.

WAN-Bandbreite Outbound (raus) - Hier können Sie die Verbindungsgeschwindigkeit des WANs für ausgehende Daten einstellen. Wenn Ihr ADSL beispielsweise 1 Mbit/s Downstream und 256 kbit/s Upstream unterstützt, geben Sie bitte in diesem Feld 256 kbit/s ein. Der Standardwert beträgt 1.000 kbit/s.

Reservierte Bandbreite - Wird für den Gruppenindex in Form einer **reservierten**

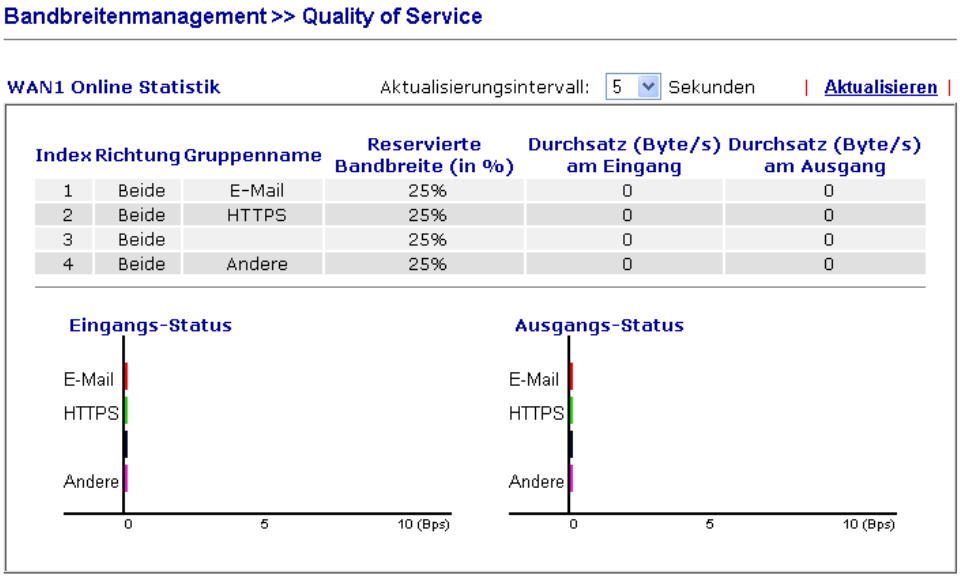
Upstream-Bandbreite und einer **reservierten Downstream-Bandbreite** reserviert.

UDP-Bandbreite begrenzen - Markieren und Bandbreitenbegrenzung im rechten Feld eingeben. Dies stellt einen Schutz für den Verkehr von TCP-Anwendungen dar, da der Verkehr von UDP-Anwendungen wie Streaming Video viel Bandbreite beansprucht.

Ausgehende TCP-ACK-Pakete priorisieren - Der Unterschied zwischen der Download- und Upload-Bandbreite ist in einer ADSL2+-Umgebung beträchtlich. Um zu vermeiden, dass die Download-Geschwindigkeit die Upload-Geschwindigkeit von ausgehenden TCP-ACK-Paketen bremst, markieren Sie dieses Kästchen, um ausgehende ACK-Pakete im Netzwerkverkehr zu beschleunigen.

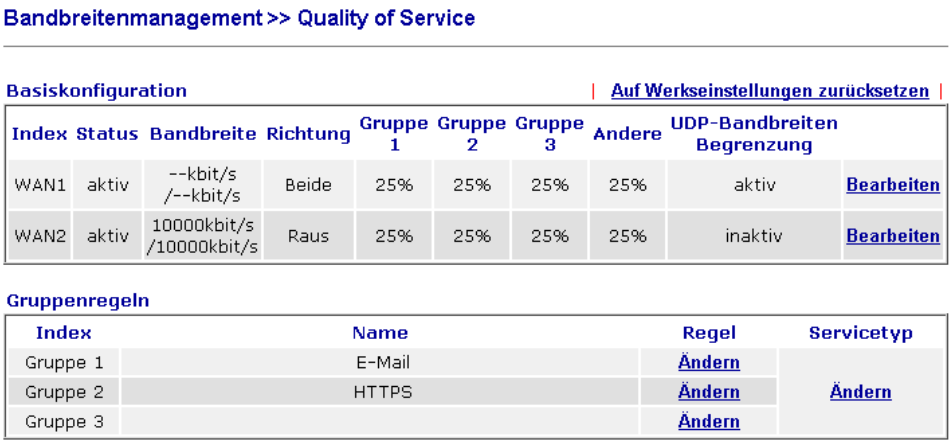
Maximale Bandbreite für UDP - Der hier eingegebene Wert wird für die maximale Bandbreite von UDP-Anwendungen verwendet.

Online-Statistik - Zeigt eine Online-Statistik der QoS an. Der Link ist nur dann sichtbar, wenn Sie in der Basiskonfiguration für WAN1/WAN2 auf **OK** klicken und dann erneut unter **Bandbreitenmanagement>>QoS** auf **Konfiguration** (für WAN1/WAN2) klicken.

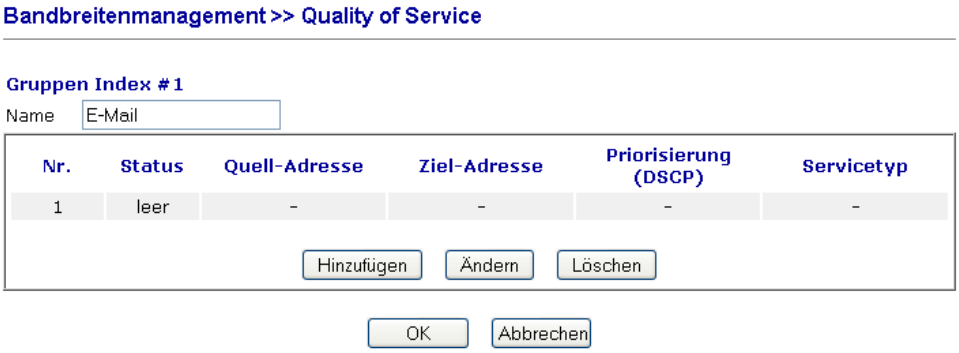


Bearbeiten der Klassenregeln für QoS

Die ersten drei Klassenregeln (Klasse 1 bis Klasse 3) können Ihren Anforderungen angepasst werden. Klicken Sie auf **Bearbeiten**, um eine Klasse hinzuzufügen, zu bearbeiten oder zu löschen.


Bandbreitenmanagement >> Quality of Service
Basiskonfiguration
Auf Werkseinstellungen zurücksetzen
Index Status Bandbreite Richtung Gruppe 1 Gruppe 2 Gruppe 3 Andere UDP-Bandbreiten Begrenzung
WAN1 aktiv --kbit/s /--kbit/s Beide 25% 25% 25% 25% aktiv Bearbeiten
WAN2 aktiv 10000kbit/s /10000kbit/s Raus 25% 25% 25% 25% inaktiv Bearbeiten
Gruppenregeln
Index Name Regel Servicetyp
Gruppe 1 E-Mail Ändern
Gruppe 2 HTTPS Ändern Ändern
Gruppe 3 Ändern

Wenn Sie auf **Bearbeiten** klicken, sehen Sie die folgende Seite. Sie können nun für die Klasse eine Bezeichnung eingeben. In diesem Fall wird "Test" als Bezeichnung für den Klassenindex Nr. 1 verwendet.


Bandbreitenmanagement >> Quality of Service
Gruppen Index #1
Name E-Mail
Nr. Status Quell-Adresse Ziel-Adresse Priorisierung (DSCP) Servicetyp
1 leer - - - -
Hinzufügen Ändern Löschen
OK Abbrechen

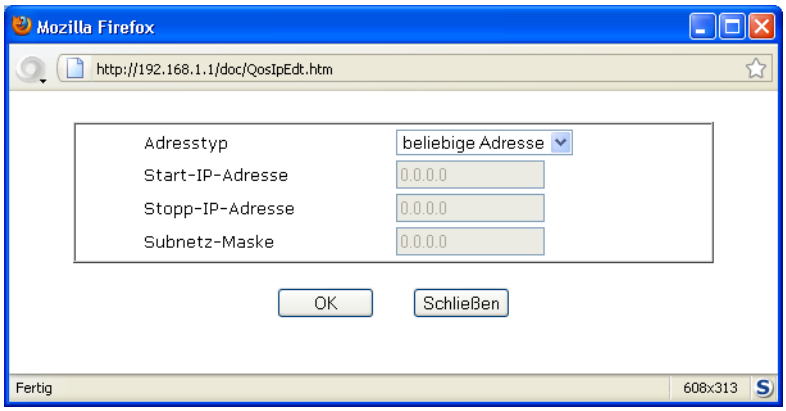
Um eine neue Regel hinzuzufügen, klicken Sie auf **Hinzufügen**, wodurch sich die folgende Seite öffnet.

ACT - Markieren Sie dieses Kästchen, um diese Einstellungen zu aktivieren.

Quell-Adresse - Klicken Sie auf **Bearbeiten**, um die lokale IP-Adresse (im LAN) für die Regel zu setzen.

Ziel-Adresse - Klicken Sie auf **Bearbeiten**, um die entfernte IP-Adresse (im LAN/WAN) für die Regel zu setzen.

Bearbeiten - Hier können Sie die Quell-Adresse bearbeiten.



Adresstyp – Bestimmen Sie den Adresstyp der Quell-Adresse.

Für eine **Einzelne Adresse** füllen Sie das Feld für die Start-IP aus.

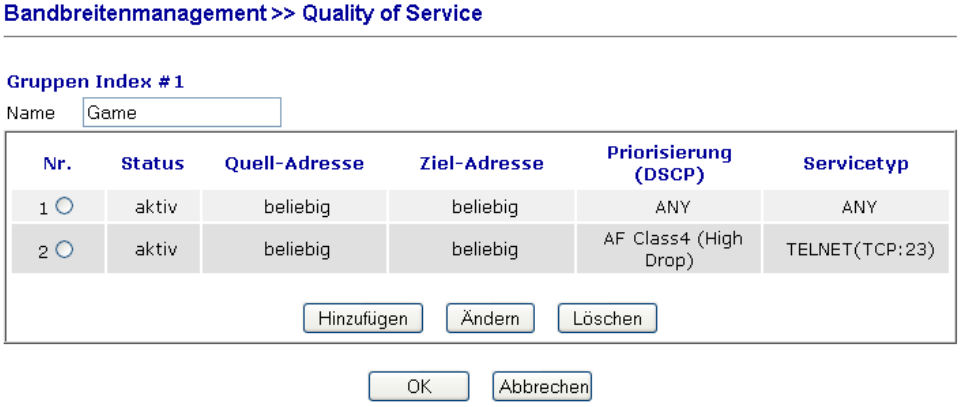
Für einen **Adressbereich** geben Sie die Start-IP und die End-IP ein.

Für eine **Subnetz-Adresse** füllen Sie die Felder für die Start-IP und Subnetz-Maske aus.

Priorisierung (DSCP) - Alle Datenpakete werden unterschiedlich eingestuft und vom System entsprechend verarbeitet. Bitte weisen Sie den Daten für die Verarbeitung mit QoS-Kontrolle eine Stufe zu.

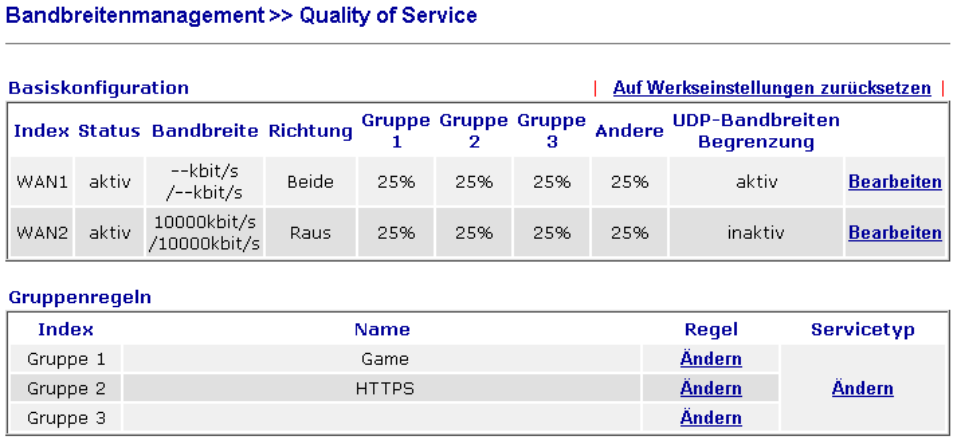
Servicetyp - Bestimmt den Servicetyp der Daten für die Verarbeitung mit QoS-Kontrolle. Dieser kann auch bearbeitet werden. Sie können einen vordefinierten Servicetyp aus der Dropdown-Liste der Servicetypen wählen. Diese Typen werden ab Werk vordefiniert. Wählen Sie einfach denjenigen, der vom aktuellen QoS verwendet werden soll.

Sie können je Klasse bis zu 20 Regeln einrichten. Um eine bestehende Regel zu bearbeiten, wählen Sie bitte den entsprechenden Eintrag und klicken auf **Bearbeiten**, um die Seite für die Änderung der Regel zu öffnen.

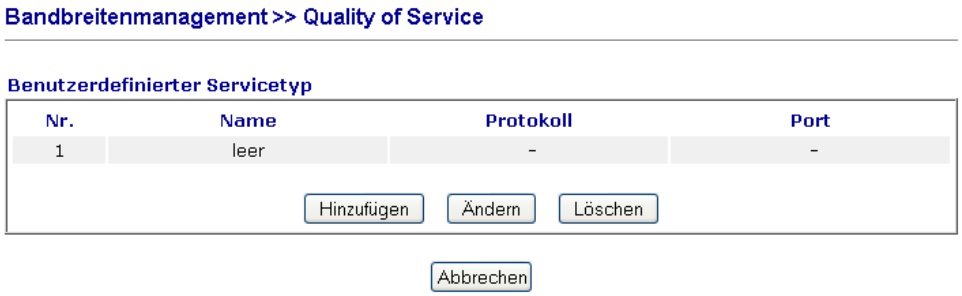


Bearbeiten der Servicetypen für die Klassenregeln

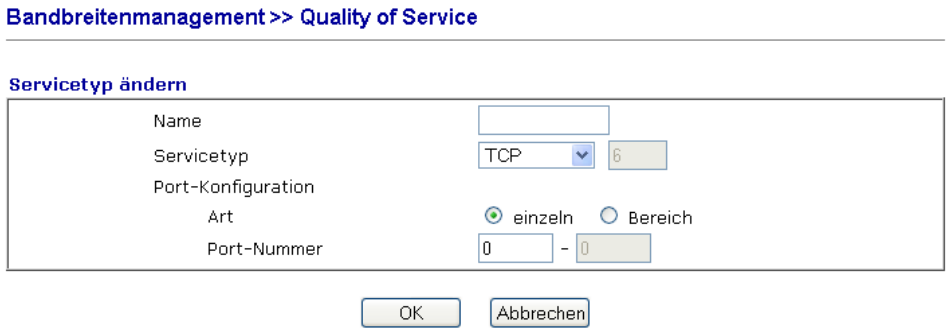
Bitte klicken Sie unter Servicetyp auf Konfiguration, um einen Servicetyp hinzuzufügen, zu bearbeiten oder zu entfernen.


Bandbreitenmanagement >> Quality of Service
Basiskonfiguration
Auf Werkseinstellungen zurücksetzen
Index Status Bandbreite Richtung Gruppe 1 Gruppe 2 Gruppe 3 Andere UDP-Bandbreiten Begrenzung
WAN1 aktiv --kbit/s /--kbit/s Beide 25% 25% 25% 25% aktiv Bearbeiten
WAN2 aktiv 10000kbit/s /10000kbit/s Raus 25% 25% 25% 25% inaktiv Bearbeiten
Gruppenregeln
Index Name Regel Servicetyp
Gruppe 1 Game Ändern
Gruppe 2 HTTPS Ändern Ändern
Gruppe 3 Ändern

Wenn Sie auf **Bearbeiten** klicken, sehen Sie die folgende Seite:



Um einen neuen Servicetyp hinzuzufügen, klicken Sie auf **Hinzufügen**, wodurch sich die folgende Seite öffnet.



Bezeichnung - Geben Sie Ihren Bedürfnissen entsprechend einen neuen Service ein.

Servicetyp - Wählen Sie den Typ (TCP, UDP oder TCP/UDP) für den neuen Dienst.

Port-Konfiguration - Wählen Sie **Einzeln** oder **Bereich** als **Typ**. Falls Sie Bereich wählen, müssen Sie in den Feldern unten den Start-Port und den End-Port eingeben.

Port-Nummer – Falls Sie als Typ **Bereich** gewählt haben, geben Sie den Start-Port und den End-Port hier ein.

Sie können bis zu 40 Servicetypen einrichten. Um einen bestehenden Servicetyp zu bearbeiten oder zu löschen, wählen Sie bitte einen Eintrag und klicken auf **Bearbeiten**.

5.8 Anwendungen

Die folgende Abbildung zeigt die Menüeinträge für Anwendungen:

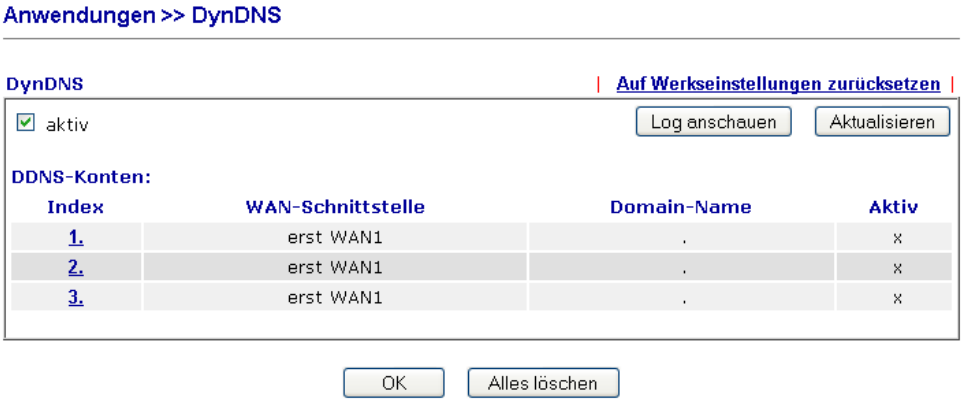
5.8.1 Dynamisches DNS

Der ISP weist Ihnen meistens eine dynamische IP-Adresse zu, mit der Sie sich über Ihren ISP mit dem Internet verbinden können. Dies bedeutet, dass sich die Ihrem Router zugewiesene öffentliche IP-Adresse in gewissen Abständen ändert. Die dynamische DNS-Funktion ermöglicht Ihnen, einer dynamischen WAN-IP-Adresse einen Domain-Namen zuzuweisen. So kann der Router seine Online-WAN-IP-Adresszuweisungen auf dem angegebenen DDNS-Server aktualisieren. Wenn der Router online ist, ist es möglich, anhand des registrierten Domain-Namens aus dem Internet auf den Router oder auf die internen virtuellen Server zuzugreifen. Dies ist besonders dann sinnvoll, wenn Sie hinter dem Router einen Web-Server, FTP-Server oder andere Server betreiben.

Bevor Sie die dynamische DNS-Funktion nutzen können, müssen Sie vom DDNS-Anbieter die Freischaltung des DDNS-Dienstes beantragen. Der Router ermöglicht die Einrichtung von bis zu drei Konten bei drei verschiedenen DDNS-Anbietern. Grundsätzlich sind Vigor-Router mit den DDNS-Diensten der beliebtesten DDNS-Anbieter kompatibel, z.B. **www.dyndns.org, www.no-ip.com, www.dtdns.com, www.changeip.com, www.dynamic-nameserver.com.** Besuchen Sie deren Web-Sites, um Ihren Domain-Namen für den Router zu registrieren.

Funktion aktivieren und dynamisches DNS-Konto hinzufügen

1. Nehmen wir an, der bei Ihrem DDNS-Anbieter registrierte Domain-Name ist *hostname.dyndns.org*, und Sie haben ein Konto mit dem Benutzernamen *test* und dem Passwort *test*.
2. Markieren Sie im DDNS-Konfigurationsmenü den Punkt **Aktiv**.



Auf Werkseinstellungen zurücksetzen - Alle Profile löschen und Werkseinstellungen wiederherstellen.

Aktiv - Markieren Sie dieses Kästchen, um die DDNS-Funktion zu aktivieren.

Index - Klicken Sie auf eine Nummer unter Index, um auf die DDNS-Konfigurationsseite zu gelangen.

WAN-Schnittstelle - Aktuelle WAN-Schnittstelle anzeigen, die für die Einwahl ins Internet verwendet wird.

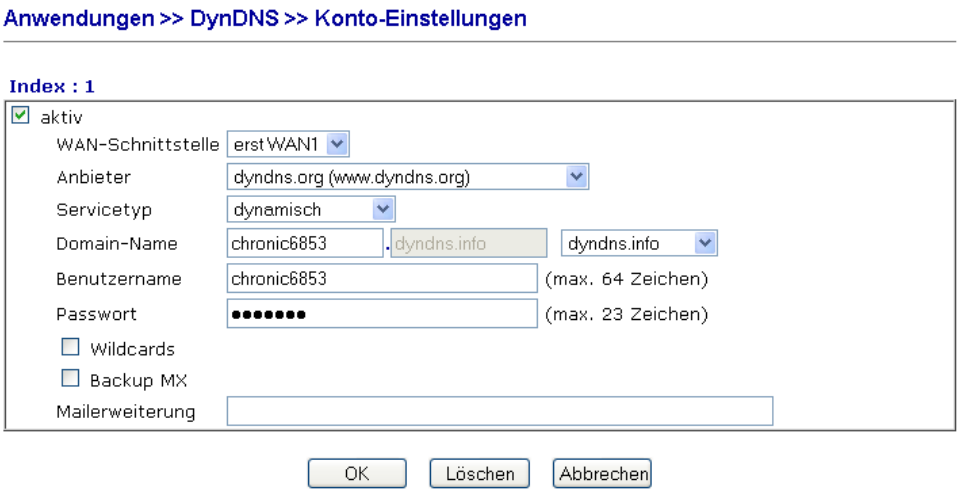
Domain-Name - Domain-Namen anzeigen, den Sie auf der Seite mit den DDNS-Einstellungen eingegeben haben.

Aktiv - Anzeigen, ob dieses Konto aktiv oder inaktiv ist.

Log ansehen - DDNS-Log-Status anzeigen.

Aktualisieren - Zwingt den Router, seine Information mit dem DDNS-Server zu aktualisieren.

3. Wählen Sie Indexnummer 1, um ein Konto für den Router hinzuzufügen. Markieren Sie **Aktiv**, wählen Sie dyndns.org als Anbieter und geben Sie den registrierten Hostnamen *hostname* und den Domain-Namenssuffix dyndns.org unter **Domain-Name** ein.



Aktiv - Markieren Sie dieses Kästchen, um das aktuelle Konto zu aktivieren. Wenn Sie dieses Kästchen aktiviert haben, erscheint in der Spalte "Aktiv" im vorherigen Dialog von Schritt 2. ein Häkchen.

WAN-Schnittstelle - Wählen Sie die WAN-Schnittstelle, auf welcher die Einstellungen angewendet werden sollen.

Anbieter - Wählen Sie den Anbieter für das DDNS-Konto

Servicetyp - Wählen Sie einen Servicetyp (dynamisch, benutzerdefiniert oder statisch). Falls Sie "benutzerdefiniert" wählen, können Sie die Domain ändern, die im Feld "Domain-Name" gewählt ist.

Domain-Name - Geben Sie einen Domain-Namen ein, den Sie zuvor konfiguriert haben. Verwenden Sie die Dropdown-Liste, um die gewünschte Domain zu wählen.

Benutzername - Geben Sie den Benutzernamen ein, den Sie für die Domain konfiguriert haben.

Passwort - Geben Sie das Passwort ein, das Sie für die Domain gesetzt haben.

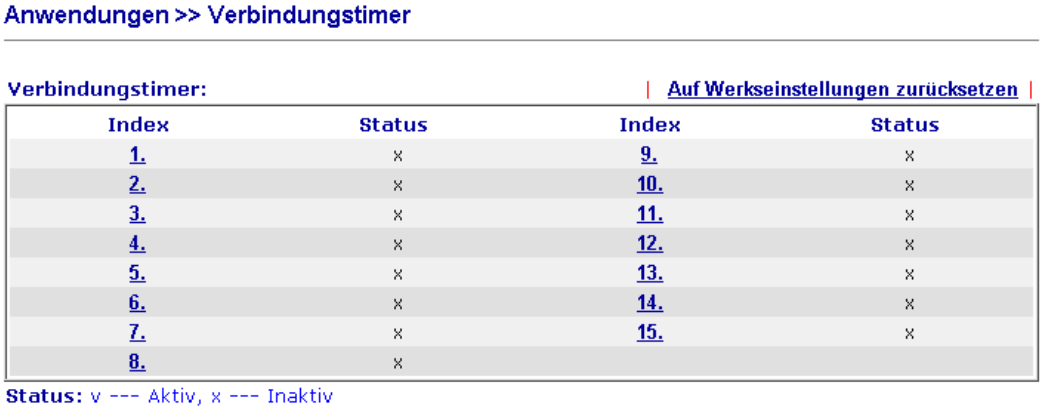
4. Klicken Sie auf **OK**, um die Einstellungen zu aktivieren. Ihre Einstellungen werden gespeichert.

Die Wildcard- und Backup MX-Funktionen werden nicht von allen DDNS-Anbietern unterstützt. Weitere Informationen sind auf den entsprechenden Web-Sites der Anbieter verfügbar.

5.8.2 Verbindungstimer

Der Vigor-Router verfügt über eine Echtzeituhr, die manuell oder automatisch über NTP (Network Time Protocol) aktualisiert werden kann. So können Sie nicht nur die Zeiten bestimmen, zu denen der Router eine Verbindung mit dem Internet aufbauen soll, sondern auch den Zugang zum Internet so beschränken, dass Benutzer nur zu bestimmten Zeiten (z.B. Öffnungszeiten) Zugriff auf das Internet haben. Der Timer kann auch für andere Funktionen verwendet werden.

Vor Einrichtung des Timers müssen Sie die Uhrzeit richtig einstellen. Klicken Sie unter **Systemmanagement>> Zeit und Datum** auf **Zeit abrufen**, um die Uhr des Vigor-Routers auf die aktuelle Zeit Ihres Rechners zu setzen. Die Uhr wird zurückgesetzt, wenn Sie den Router ausschalten oder auf die Werkseinstellungen zurücksetzen. Es gibt auch eine andere Methode, um die Uhrzeit abzufragen. Sie können die Router-Zeit mit einem NTP-Server (Zeitserver) im Internet synchronisieren. Allerdings ist dies erst möglich, nachdem eine WAN-Verbindung aufgebaut wurde.



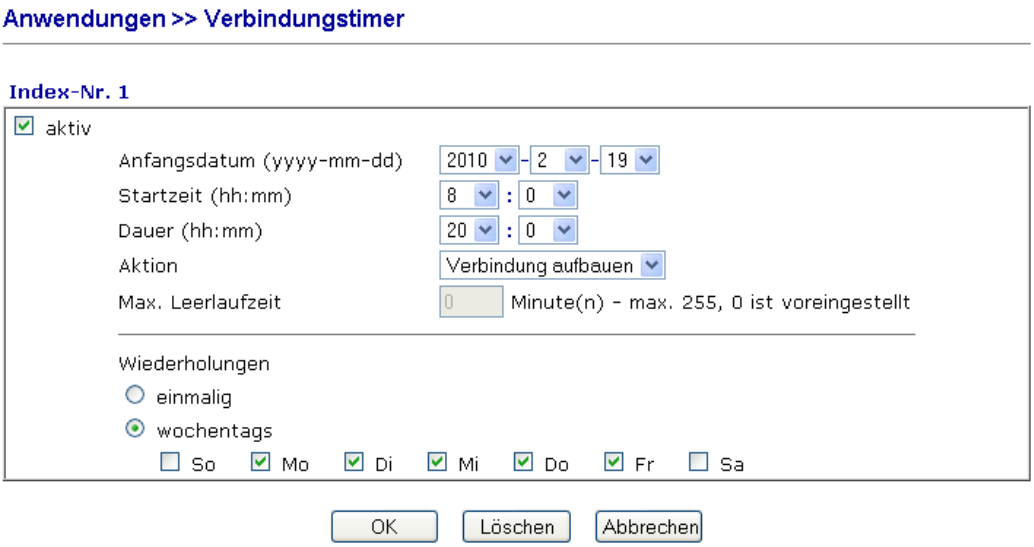
Auf Werkseinstellungen zurücksetzen - Alle Profile löschen und Werkseinstellungen wiederherstellen.

Index - Klicken Sie auf eine Nummer unter Index, um auf die Timer-Konfigurationsseite zu gelangen.

Status - Zeigt an, ob dieser Timer aktiv oder inaktiv ist.

Sie können bis zu 15 Timer einrichten. Diese können daraufhin auf die Einstellungen unter **Einwahl ins Internet** oder **VPN und externe Einwahl >> LAN-zu-LAN** angewendet werden.

Um einen Timer hinzuzufügen, klicken Sie auf einen beliebigen Index, z.B. Index Nr. 1. Die Einstellungen des Verbindungstimers unter Index 1 werden in der folgenden Abbildung detailliert dargestellt.



Aktiv - Markieren Sie dieses Kästchen, um den Timer zu aktivieren.

Anfangsdatum (yyyy-mm-dd) - Anfangsdatum des Timers angeben.

Startzeit (hh:mm) Startzeit des Timers angeben.

Dauer (hh:mm) - Geben Sie die Dauer (oder den Zeitraum) für den Timer an.

Aktion - Geben Sie die Aktion an, die der Verbindungstimer während des Timer-Zeitraums ausführen soll.

Verbindung aufbauen -Verbindung ständig aufrecht erhalten.

Verbindung beenden - Verbindung ständig inaktiv halten.

Einwahl zulassen - Erlauben Sie den Verbindungsaufbau bei Bedarf und geben Sie die Zeit, nachdem die Verbindung abgebrochen werden soll, unter **Max. Leerlaufzeit** an.

Einwahl unterbinden - Erhält die Verbindung aufrecht, solange über die Leitung Datenaustausch stattfindet. Nach der maximalen Leerlaufzeit ohne Datenaustausch wird die Verbindung abgebrochen und die erneute Einwahl während des Timer-Zeitraums unterbunden.

Max. Leerlaufzeit - Geben Sie die Dauer (oder den Zeitraum) für den Timer an.

Wiederholungen - Geben Sie an, wie oft der Timer wiederholt werden soll.

Einmalig - Der Timer kommt nur einmal zur Anwendung.

Wochentags - Geben Sie die Wochentage an, an denen der Zeitplan angewendet werden soll.

Beispiel

Angenommen, Sie möchten, dass die PPPoE-Internetverbindung während der ganzen Woche von 9:00 Uhr bis 18:00 aktiv ist. Zu anderen Zeiten soll die Internetverbindung nicht aktiv sein (Verbindung beenden).

Bürozeit:

(Verbindung aufbauen)

Mo - So9:00 Uhr bis 18:00 Uhr

7. Die PPPoE-Verbindung muss ordnungsgemäß funktionieren und **Zeit und Datum** müssen richtig eingestellt sein.

8. Richten Sie das System so ein, dass PPPoE jeweils die ganze Woche von 9:00 bis 18:00 verfügbar ist.

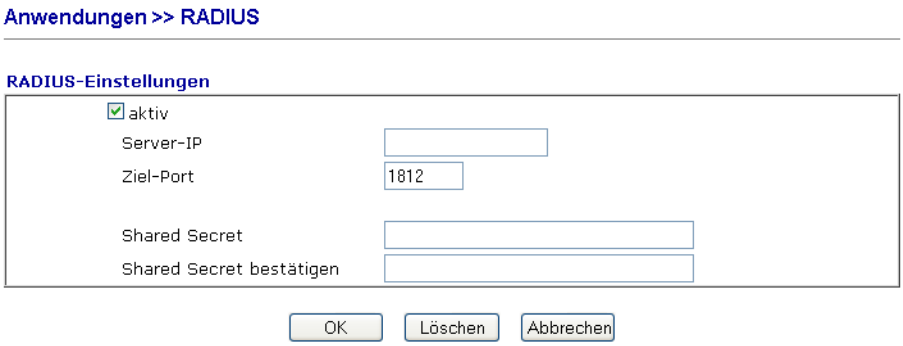
9. Konfigurieren Sie die Aktion **Verbindung beenden** so, dass die Verbindung während der ganzen Woche von 18:00 Uhr bis zum nächsten Tag um 9:00 Uhr nicht verfügbar ist.

10. Weisen Sie diese beiden Profile dem PPPoE-Internet-Einwahlprofil zu. Der Router wird gemäß den voreingestellten Timer-Profilen die **Verbindung aufbauen** oder die **Verbindung beenden**.

5.8.3 RADIUS

RADIUS (Remote Authentication Dial-In User Service) ist ein Client-Server-Protokoll, das zur sicheren Authentifizierung, Autorisierung und zum Accounting dient, und wird von vielen ISPs verwendet. Es ist die am weitesten verbreitete Methode für die Authentifizierung und Autorisierung von Einwahl- und Tunnelverbindungen von Netzwerkbenutzern.

Die eingebaute RADIUS Client-Funktionalität ermöglicht dem Router, den externen Benutzer oder einen WLAN-Client und den RADIUS-Server bei der gegenseitigen Authentifizierung zu unterstützen. Die Funktionalität ermöglicht zentralisierte Fernzugriffsauthentifizierung für Netzwerkmanagement.



Aktiv - Markieren Sie dieses Kästchen, um die RADIUS-Client-Funktionalität zu aktivieren.

Server-IP - Geben Sie die IP-Adresse des RADIUS-Servers ein.

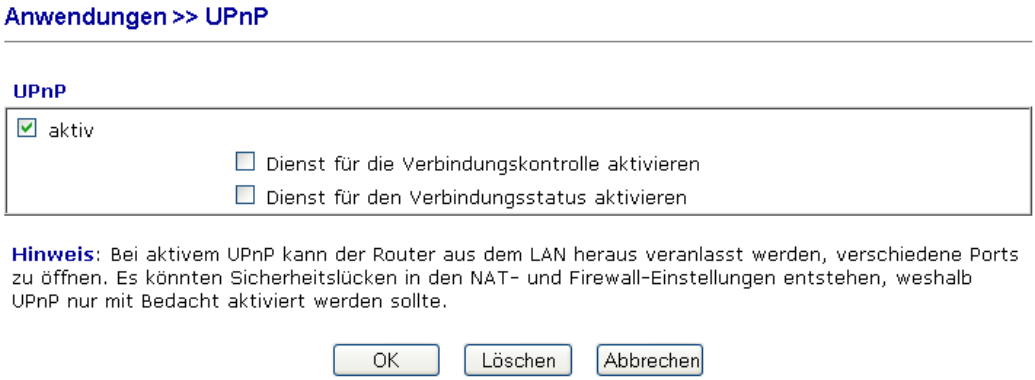
Ziel-Port - Die vom RADIUS-Server verwendete UDP-Port-Nummer. Der Standardwert gemäß RFC 2138 ist 1812.

Shared Secret - Der RADIUS-Server und der Client teilen sich ein Passwort (Shared Secret) mit, das verwendet wird, um die zwischen ihnen kommunizierten Meldungen zu authentifizieren. Beide Seiten müssen so konfiguriert werden, dass sie das gleiche Shared Secret verwenden.

Shared Secret bestätigen - Bestätigen Sie das Shared Secret durch erneute Eingabe.

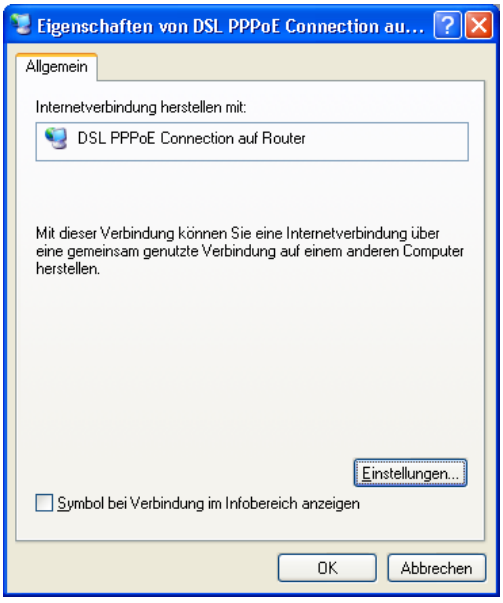
5.8.4 UPnP

Das **UPnP**-Protokoll (Universal Plug and Play) wird unterstützt, um die Installation und Konfiguration von Netzwerkgeräten zu vereinfachen, wie dies bereits bei direkt angeschlossenen PC-Peripheriegeräten mit dem Windows "Plug and Play"-System der Fall ist. Bei NAT-Routern ist "NAT-Traversal" die wichtigste UPnP-Funktion des Routers. Sie ermöglicht Anwendungen hinter der Firewall, automatisch die Ports zu öffnen, die für die Weiterleitung durch einen Router erforderlich sind. Dies ist verlässlicher, als den Router selbst feststellen zu lassen, welche Ports geöffnet werden müssen. Außerdem muss der Benutzer keine Port-Zuordnungen oder DMZ manuell einrichten. **UPnP ist für Windows XP verfügbar**, und der Router bietet die entsprechende Unterstützung für MSN Messenger, um die Verwendung der Sprach-, Video- und Messaging-Funktionen uneingeschränkt zu ermöglichen.

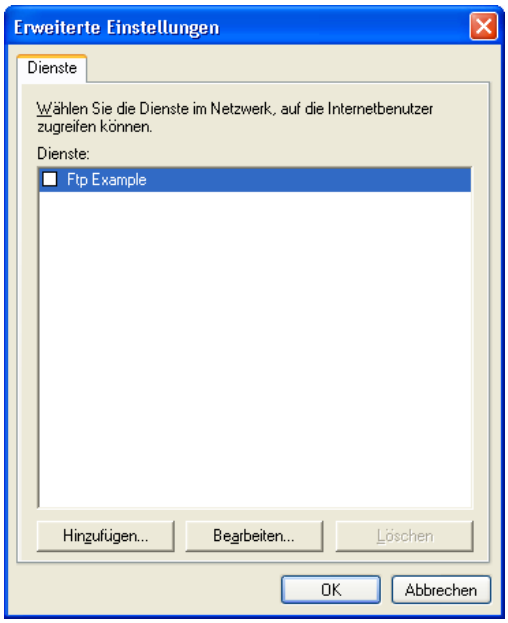

Anwendungen >> UPnP
UPnP
aktiv
Dienst für die Verbindungskontrolle aktivieren
Dienst für den Verbindungsstatus aktivieren
Hinweis: Bei aktivem UPnP kann der Router aus dem LAN heraus veranlasst werden, verschiedene Ports zu öffnen. Es könnten Sicherheitslücken in den NAT- und Firewall-Einstellungen entstehen, weshalb UPnP nur mit Bedacht aktiviert werden sollte.
OK
Löschen
Abbrechen

Aktiv — Sie können entweder den Dienst für die **Verbindungskontrolle** oder den Dienst für den **Verbindungsstatus** aktivieren.

Nachdem diese Funktion auf **Aktiv** gesetzt wurde, erscheint unter Windows XP/Netzwerkverbindungen das Symbol **IP-Breitbandverbindung auf Router**. Der Verbindungsstatus und der Verbindungskontrollstatus können aktiviert werden. Die NAT-Traversal-Funktion von UPnP ermöglicht die Verwendung der Multimedia-Funktionen Ihrer Anwendungen. Die Port-Zuordnungen müssen manuell oder anderweitig eingestellt werden. Die folgenden Screenshots zeigen anhand von Beispielen, wie dies funktioniert.


Eigenschaften von DSL PPPoE Connection au...
Allgemein
Internetverbindung herstellen mit:
DSL PPPoE Connection auf Router
Mit dieser Verbindung können Sie eine Internetverbindung über eine gemeinsam genutzte Verbindung auf einem anderen Computer herstellen.
Einstellungen...
Symbol bei Verbindung im Infobereich anzeigen
OK
Abbrechen

Die UPnP-Funktion des Routers ermöglicht Anwendungen mit UPnP-Unterstützung wie MSN Messenger, zu erkennen, was sich hinter einem NAT-Router befindet. Die Anwendung erkennt auch die externe IP-Adresse und konfiguriert die Port-Zuordnungen auf dem Router. Danach ermöglicht diese Funktion die Weiterleitung von Paketen von den externen Ports des Routers zu den internen Ports, die von der Anwendung verwendet werden.



Hinweis zur Firewall und UPnP

Probleme mit Firewall-Software

Der Einsatz von Firewall-Anwendungen auf Ihrem Rechner kann die UPnP-Funktion behindern. Dies liegt daran, dass diese Anwendungen den Zugriff auf einige Netzwerk-Ports blockieren.

Sicherheitsüberlegungen

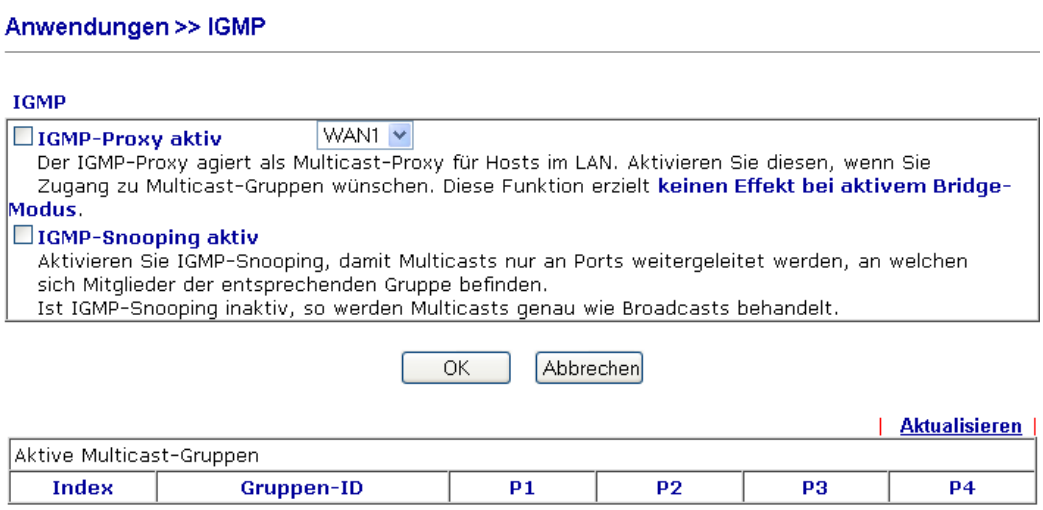
Die Verwendung der UPnP-Funktion in Ihrem Netzwerk kann gewisse Sicherheitsrisiken mit sich bringen. Sie sollten diese Risiken genau abwägen, bevor Sie die UPnP-Funktion aktivieren.

- Da die Schwächen der UPnP-Funktion bei manchen Microsoft-Betriebssystemen ausgenutzt werden können, ist es wichtig, die neuesten Service Packs und Patches einzuspielen.
- Nicht privilegierte Benutzer können gewisse Router-Funktionen steuern, z.B. Port-Zuordnungen entfernen und hinzufügen.

Die UPnP-Funktion fügt dynamisch Port-Zuordnungen für einige Anwendungen mit UPnP-Unterstützung hinzu. Falls diese Anwendungen abstürzen, kann es sein, dass diese Zuordnungen nicht entfernt werden.

5.8.5 IGMP

IGMP ist die Abkürzung für *Internet Group Management Protocol*. Es handelt sich hierbei um ein Kommunikationsprotokoll, das hauptsächlich für die Verwaltung der Mitgliedschaft in Internet-Protokoll-Multicast-Gruppen zum Einsatz kommt. Um die IGMP-Snooping-Funktion zu verwenden, markieren Sie zunächst das Kästchen IGMP-Proxy aktiv, um die IGMP-Proxy-Funktion zu aktivieren.


Anwendungen >> IGMP
IGMP
IGMP-Proxy aktiv
WAN1
Der IGMP-Proxy agiert als Multicast-Proxy für Hosts im LAN. Aktivieren Sie diesen, wenn Sie Zugang zu Multicast-Gruppen wünschen. Diese Funktion erzielt keinen Effekt bei aktivem Bridge-Modus.
IGMP-Snooping aktiv
Aktivieren Sie IGMP-Snooping, damit Multicasts nur an Ports weitergeleitet werden, an welchen sich Mitglieder der entsprechenden Gruppe befinden.
Ist IGMP-Snooping inaktiv, so werden Multicasts genau wie Broadcasts behandelt.
OK
Abbrechen
Aktualisieren
Aktive Multicast-Gruppen
Index
Gruppen-ID
P1
P2
P3
P4

IGMP-Proxy aktiv - Markieren Sie dieses Kästchen, um diese Funktion zu aktivieren. Die Multicast-Anwendung wird über den angegebenen WAN-Port ausgeführt.

IGMP-Snooping aktiv - Markieren Sie dieses Kästchen, um diese Funktion zu aktivieren. Die Multicast-Anwendung wird für die Clients im LAN ausgeführt.

Gruppen-ID - Dieses Feld zeigt den ID-Port für die Multicast-Gruppe an. Der verfügbare Bereich für IGMP reicht von 224.0.0.0 bis 255.255.254.

P1 bis P4 - Zeigt den LAN-Port an, der für die Multicast-Gruppe verwendet wird.

Aktualisieren - Klicken Sie hier, um den Status der Multicast-Gruppe zu aktualisieren.

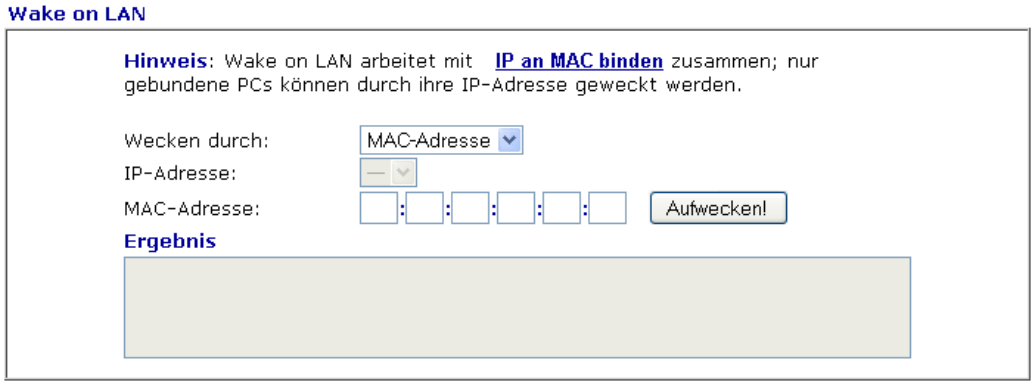
Markieren Sie IGMP-Proxy aktiv, um auf die folgende Seite zu gelangen. Es werden alle Multicast-Gruppen und alle verfügbaren LAN-Ports (P1 bis P4) aufgeführt.

5.8.6 Wake on LAN

Ein mit dem LAN verbundener Rechner kann vom Router aufgeweckt werden. Um einen bestimmten Rechner über den Router aufzuwecken, muss die korrekte MAC-Adresse des jeweiligen Rechners in diesem Dialog angegeben werden.

Außerdem muss der Rechner über eine Netzwerkkarte verfügen, welche die WOL-Funktion unterstützt. Die WOL-Funktion muss im BIOS des jeweiligen Rechners aktiviert werden.

Anwendungen >> Wake on LAN



Wecken durch: - Ein Gerät kann auf zweierlei Weise aufgeweckt werden. Falls Sie Wecken durch MAC-Adresse wählen, müssen Sie die korrekte MAC-Adresse des Hosts im MAC-Adressfeld eingeben. Falls Sie Wecken durch IP-Adresse wählen, müssen Sie die richtige IP-Adresse bestimmen.

IP-Adresse - Die IP-Adressen, die unter **Firewall>>IP an MAC binden** vorhanden sind, erscheinen in dieser Dropdown-Liste. Wählen Sie die IP-Adresse, welche Sie aufwecken möchten, aus der Dropdown-Liste.

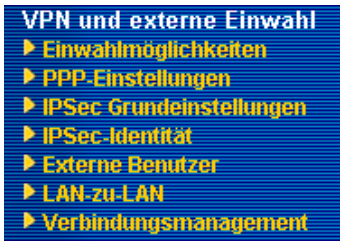
MAC-Adresse - Geben Sie die MAC-Adresse eines gebundenen PCs an.

Aufwecken! - Klicken Sie auf diese Taste, um die ausgewählte IP aufzuwecken. Sehen Sie die folgende Abbildung. Das Ergebnis wird im Feld angezeigt.

5.9 VPN und externe Einwahl

Ein VPN (Virtual Private Network) ist die Erweiterung eines privaten Netzwerks, dass Verbindungen über gemeinsame bzw. öffentliche Netzwerke wie das Internet ermöglicht. Die Übertragung von Daten zwischen zwei Rechnern über ein gemeinsames bzw. öffentliches Netzwerk mit der VPN-Technologie entspricht den Eigenschaften einer privaten P2P-Verbindung.

Die folgende Abbildung zeigt die Menüeinträge für VPN und Fernzugriff:



5.9.1 Einwahlmöglichkeiten

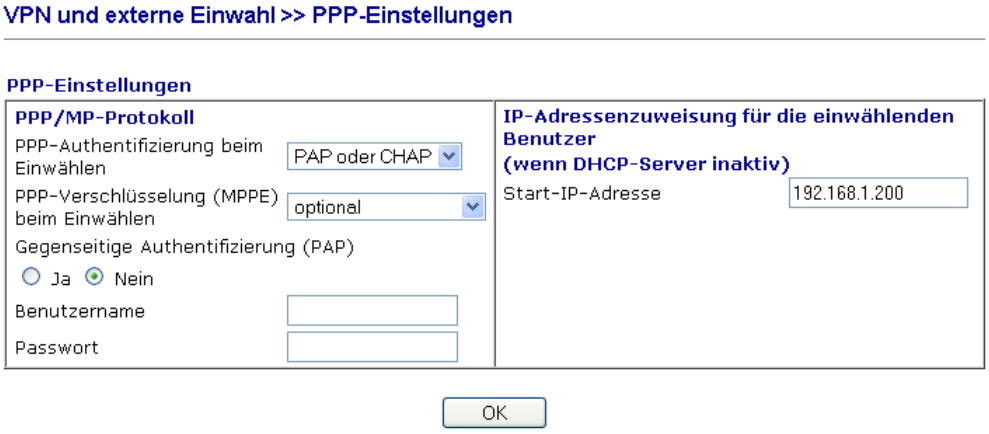
Aktivieren Sie bei Bedarf den erforderlichen VPN-Dienst. Falls Sie beabsichtigen, in Ihrem LAN einen VPN-Server zu betreiben, sollten Sie den VPN-Dienst des Vigor-Routers deaktivieren, damit die Datenpakete den VPN-Tunnel passieren können, und die entsprechenden NAT-Einstellungen vornehmen (DMZ, Ports öffnen).

VPN und externe Einwahl >> Einwahlmöglichkeiten
Einwahlmöglichkeiten
PPTP
IPSec
L2TP
ISDN
Hinweis: Wenn Sie einen VPN-Server in Ihrem LAN betreiben wollen, müssen Sie die entsprechenden Protokolle oben deaktivieren. Nur so können die Datenpakete uneingeschränkt passieren. Außerdem sollten Sie die verwendeten Ports für den VPN-Server in den NAT- und Firewall-Einstellungen des Routers öffnen.
OK
Löschen
Abbrechen

Der Vigor-Router akzeptiert keine ISDN-Einwahlverbindungen, falls das Kästchen **ISDN** nicht markiert ist.

5.9.2 PPP-Einstellungen

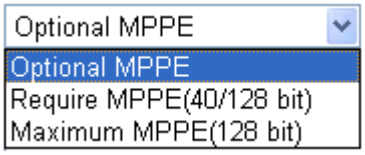
Dieses Untermenü wird nur für PPP-bezogene VPN-Verbindungen wie PPTP, L2TP und L2TP over IPSec benötigt.



PPP-Authentifizierung beim Einwählen Nur PAP - Wählen Sie diese Option, damit der Router Einwahlbenutzer über das PAP-Protokoll authentifiziert.

PAP oder CHAP - Wählen Sie diese Option, so versucht der Router zunächst, Einwahlbenutzer über das CHAP-Protokoll zu authentifizieren. Falls der Einwahlbenutzer dieses Protokoll nicht unterstützt, wird für die Authentifizierung auf das PAP-Protokoll zurückgegriffen.

PPP-Verschlüsselung (MPPE) beim Einwählen Optional - Wird diese Option gewählt, verwendet der Router optional die MPPE-Verschlüsselungsmethode für externe Benutzer. Falls der externe Benutzer den MPPE-Verschlüsselungsalgorithmus nicht unterstützt, versendet der Router keine MPPE-verschlüsselten Pakete. Ansonsten werden die Daten mit MPPE verschlüsselt.



Benötigt (40/128 bit) - Die Auswahl dieser Option zwingt den Router, Pakete mit dem MPPE-Algorithmus zu verschlüsseln. Der externe Benutzer setzt zunächst 40-Bit-Verschlüsselung ein, bevor 128-Bit-Verschlüsselung zum Einsatz kommt. Falls 128-Bit MPPE-Verschlüsselung nicht verfügbar ist, wird also für die Verschlüsselung der Daten 40-Bit-Verschlüsselung verwendet.

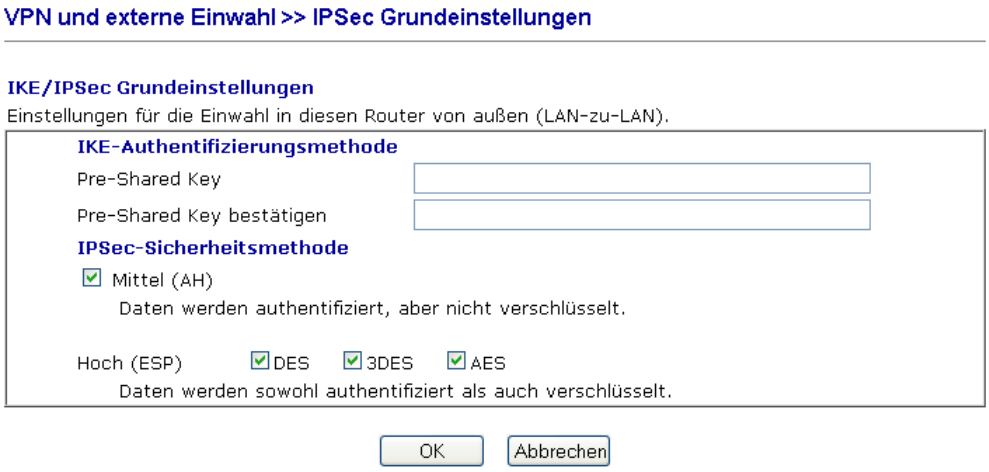
Maximal (128 bit) - Mit dieser Option verwendet der Router die MPPE-Verschlüsselung mit maximaler Bit-Anzahl (128 Bits), um die Daten zu verschlüsseln.

Gegenseitige Authentifizierung (PAP) - Die Funktion zur gegenseitigen Authentifizierung dient hauptsächlich der Kommunikation mit anderen Routern oder Clients, die zweiseitige Authentifizierung erfordern, um ein höheres Sicherheitsniveau zu erreichen (z.B. Cisco-Router). Sie sollten daher diese Funktion aktivieren, falls der andere Router dies erfordert. Geben Sie in diesem Fall den **Benutzernamen** und das **Passwort** des Peers für die gegenseitige Authentifizierung ein.

Start-IP-Adresse - Geben Sie für die PPP-Einwahlverbindung eine Start-IP ein. Wählen Sie eine IP-Adresse aus dem lokalen privaten Netzwerk. Wenn zum Beispiel das lokale private Netzwerk 192.168.1.0/255.255.255.0 ist, können Sie 192.168.1.200 als Start-IP-Adresse wählen. Beachten Sie, dass die ersten zwei IP-Adressen, 192.168.1.200 und 192.168.1.201, für entfernte ISDN-Benutzer reserviert sind.

5.9.3 IPSec Grundeinstellungen

In den **IPSec Grundeinstellungen** besteht die Konfiguration aus zwei wesentlichen Teilen.



IPSec umfasst zwei Phasen:

➢ Phase 1: Aushandlung von IKE-Parametern wie Verschlüsselung, Hash, Diffie-Hellman-Parameterwerte und Gültigkeitsdauer, um den nachfolgenden IKE-Austausch zu schützen, Authentifizierung beider Peers mit Pre-Shared Key oder digitaler Signatur (x.509). Der Peer, der die Verhandlung initiiert, schlägt dem entfernten Peer alle seine Verfahren vor, und der entfernte Peer versucht, eine Übereinstimmung höchster Priorität zu finden. Schließlich wird ein sicherer Tunnel für IKE Phase 2 eingerichtet.

➢ Phase 2: Aushandlung von IPSec-Sicherheitsmethoden wie AH (Authentication Header) oder ESP (Encapsulating Security Payload) für den nachfolgenden IKE-Austausch und gegenseitige Prüfung des Aufbaus eines sicheren Tunnels.

Es werden für IPSec zwei Kapselungsmethoden verwendet: **Transport** und **Tunnel**. Der **Transport**-Modus fügt die AH-/ESP-Daten hinzu und benutzt die ursprünglichen IP-Header, um nur die Nutzdaten zu kapseln. Dies ist nur beim lokalen Paket möglich, z.B. L2TP über IPSec. Der **Tunnel**-Modus fügt nicht nur die AH-/ESP-Daten hinzu, sondern verwendet außerdem einen neuen IP-Header (Tunneled IP Header), um das

gesamte ursprüngliche IP-Paket zu kapseln.

AH (Authentication Header) bietet Datenauthentifizierung und Integrität für IP-Pakete, die zwischen den VPN-Peers ausgetauscht werden. Zu diesem Zweck wird eine verschlüsselte Einweg-Hash-Funktion auf das Paket angewendet, um einen Message Digest zu erstellen. Dieser Digest wird in den AH integriert und mit den Paketen zusammen übertragen. Auf der Empfängerseite wendet der Peer die gleiche Einweg-Hash-Funktion auf das Paket an und vergleicht den Wert mit dem Wert im empfangenen AH.

ESP (Encapsulating Security Payload) ist ein Sicherheitsprotokoll, dass Vertraulichkeit und Datenschutz mit optionaler Authentifizierung und Replay-Erkennung bietet.

IKE-Authentifizierungsmethode - Betrifft normalerweise externe Benutzer oder Knoten (LAN zu LAN), die dynamische IP-Adressen und IPSec-bezogene VPN-Verbindungen wie L2TP über IPSec und IPSec-Tunnel benutzen.

Pre-Shared Key - Zur Zeit wird nur Authentifizierung mit Pre-Shared Key für IKE unterstützt.

Pre-Shared Key bestätigen - Geben Sie die Zeichenfolge erneut ein, um den Pre-Shared Key zu bestätigen.

IPSec-SicherheitsmethodeMittel - Authentication Header (AH) bedeutet, dass die Daten authentifiziert, jedoch nicht verschlüsselt werden. Diese Option ist standardmäßig aktiviert.

Hoch - Encapsulating Security Payload (ESP) bedeutet, dass die Nutzdaten sowohl verschlüsselt als auch authentifiziert werden. Als Verschlüsselungsalgorithmus stehen DES (Data Encryption Standard), 3DES (Triple DES) und AES zur Verfügung.

5.9.4 IPSec-Identität

Um für die Peer-Authentifizierung bei LAN-zu-LAN-Verbindungen oder externen Einwahlverbindungen digitale Zertifikate zu verwenden, können Sie hier eine Liste von Peer-Zertifikaten verwalten. Wie aus der folgenden Abbildung ersichtlich, bietet der Router **32** Einträge für digitale Zertifikate für Einwahlbenutzer.

VPN und externe Einwahl >> IPSec-Identität

X.509 ID Konten: | Auf Werkseinstellungen zurücksetzen |

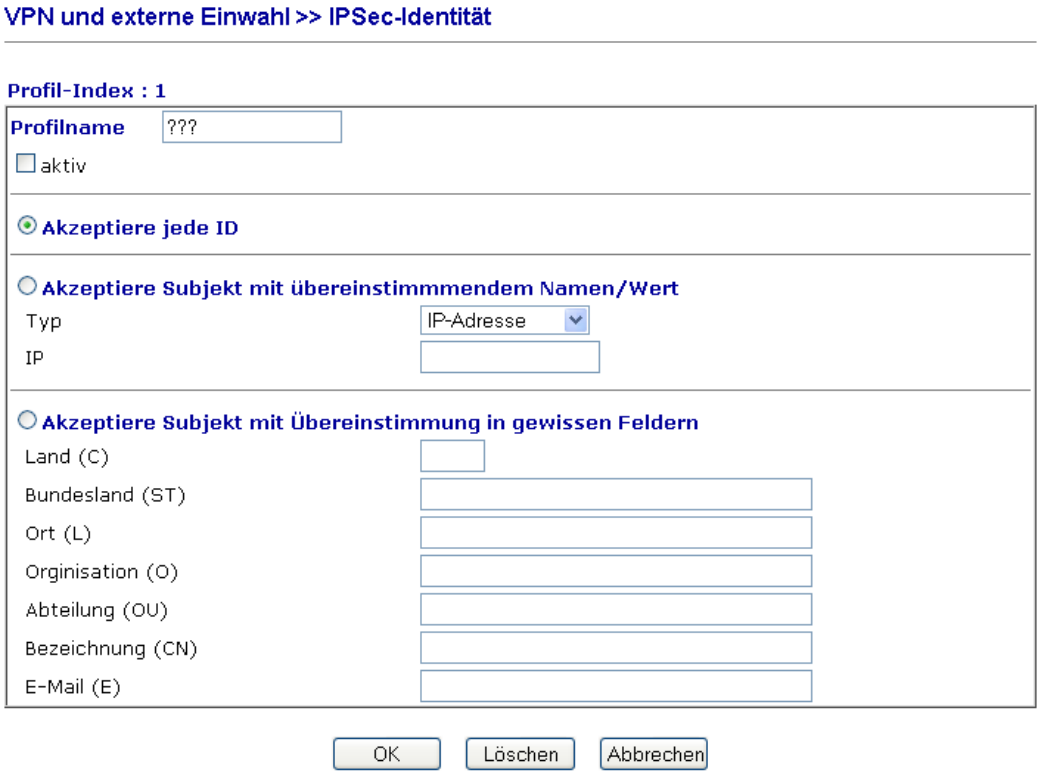
Index	Name	Status	Index	Name	Status
1.	???	X	17.	???	X
2.	???	X	18.	???	X
3.	???	X	19.	???	X
4.	???	X	20.	???	X
5.	???	X	21.	???	X
6.	???	X	22.	???	X
7.	???	X	23.	???	X
8.	???	X	24.	???	X
9.	???	X	25.	???	X
10.	???	X	26.	???	X
11.	???	X	27.	???	X
12.	???	X	28.	???	X
13.	???	X	29.	???	X
14.	???	X	30.	???	X
15.	???	X	31.	???	X
16.	???	X	32.	???	X

Auf Werkseinstellungen zurücksetzen - Klicken Sie auf diese Taste, um alle Einträge zu löschen.

Index - Klicken Sie auf eine Nummer unter Index, um auf die Konfigurationsseite für die IPSec-Identität zu gelangen.

Name - Profilnamen dieses Indexes anzeigen.

Klicken Sie auf die einzelnen Einträge, um jeweils ein digitales Peer-Zertifikat zu bearbeiten. Die Authentifizierung der digitalen Signaturen umfasst drei Sicherheitsstufen. Füllen Sie alle erforderlichen Felder aus, um den externen Peer zu authentifizieren. Die folgenden Erläuterungen werden Ihnen dabei behilflich sein, alle notwendigen Felder auszufüllen.



Profilname - Geben Sie in diesem Feld eine Bezeichnung ein.

Akzeptiere jede ID - Hier klicken, um ungeachtet der Identität jeden Peer zu akzeptieren.

Akzeptiere Subjekt mit übereinstimmendem Namen/Wert - Hier klicken, um ein bestimmtes Feld der digitalen Signatur zu markieren, mit dem der Peer übereinstimmen muss, damit er akzeptiert wird. Das Feld kann die **IP-Adresse, Domain,** oder **E-Mail-Adresse** sein. Je nach gewähltem Typ erscheint das entsprechende Feld und fordert Sie zur Eingabe auf.

Akzeptiere Subjekt mit Übereinstimmung in gewissen Feldern - Hier klicken, um die bestimmten Felder der digitalen Signatur zu markieren, mit dem der Peer übereinstimmen muss, damit er akzeptiert wird. Die Felder umfassen **Country (C), State (ST), Location (L), Organization (O), Organization Unit (OU), Common Name (CN)** und **Email (E)**.

5.9.5 Externe Benutzer

Sie können Fernzugriffe verwalten, indem Sie eine Tabelle der Profile externer Benutzer unterhalten. Diese Tabelle ermöglicht die Authentifizierung von Benutzern, die sich über ISDN oder über eine VPN-Verbindung einwählen. Sie können Parameter wie die Peer-ID, Verbindungstyp (ISDN-Einwahlverbindung, VPN-Verbindung einschl. PPTP, IPSec Tunnel und L2TP mit oder ohne IPSec), Sicherheitsmethoden usw. einstellen.

Der Router bietet **32** Zugangskonten für externe Benutzer. Durch die eingebaute RADIUS-Client-Funktion können die Benutzerkonten auch für den RADIUS-Server verwendet werden. Die folgende Abbildung zeigt eine Zusammenfassung.

VPN und externe Einwahl >> Externe Benutzer

Profile externer Benutzer: | Auf Werkseinstellungen zurücksetzen |

Index	Benutzer	Status	Index	Benutzer	Status
1.	???	X	17.	???	X
2.	???	X	18.	???	X
3.	???	X	19.	???	X
4.	???	X	20.	???	X
5.	???	X	21.	???	X
6.	???	X	22.	???	X
7.	???	X	23.	???	X
8.	???	X	24.	???	X
9.	???	X	25.	???	X
10.	???	X	26.	???	X
11.	???	X	27.	???	X
12.	???	X	28.	???	X
13.	???	X	29.	???	X
14.	???	X	30.	???	X
15.	???	X	31.	???	X
16.	???	X	32.	???	X

Auf Werkseinstellungen zurücksetzen - Klicken Sie auf diese Taste, um alle Einträge zu löschen.

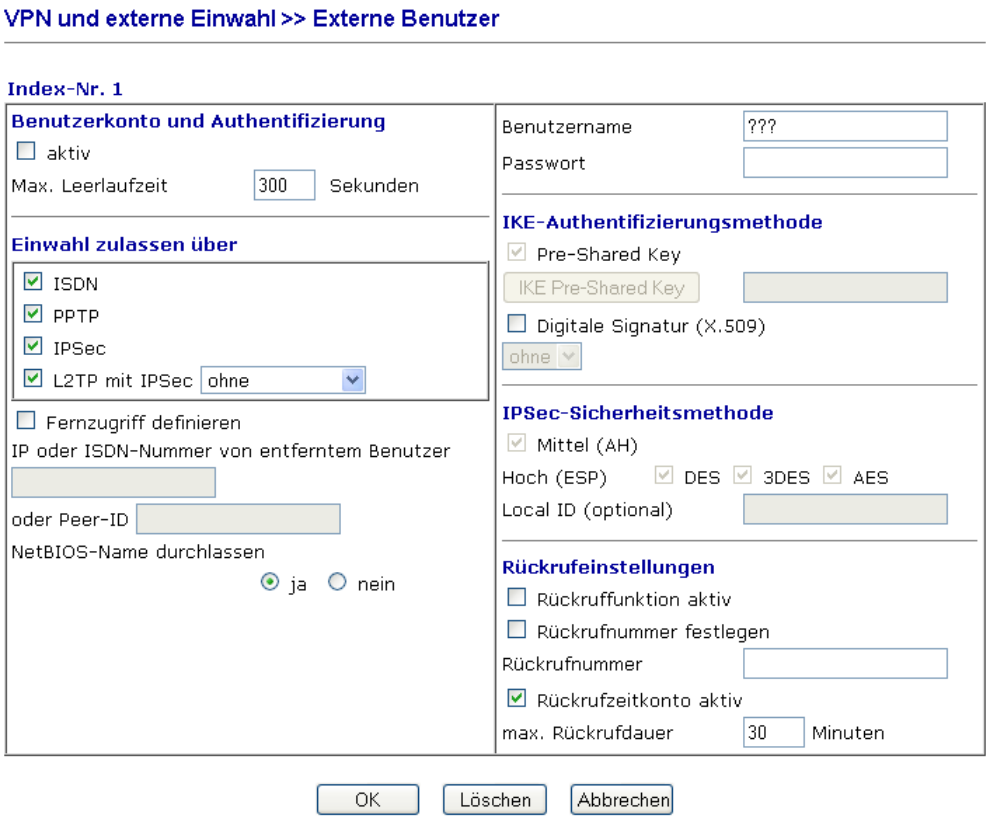
Index - Klicken Sie auf eine Nummer unter Index, um auf die Konfigurationsseite für externe Benutzer zu gelangen.

Benutzer - Zeigt den Benutzernamen des entsprechenden externen Benutzers im LAN-zu-LAN-Profil an. Die Zeichen **???** lassen erkennen, dass das Profil leer ist.

Status - Zeigt den Zugangsstatus des jeweiligen externen Benutzers an. "V" zeigt an, dass der externe Benutzer aktiv ist, während "X" anzeigt, dass er inaktiv ist.

Klicken Sie auf eine der Indexnummern, um ein externes Benutzerprofil zu bearbeiten. **Füllen Sie für jeden Einwahltyp die entsprechenden Felder rechts aus.** Ausgegraute Felder brauchen nicht ausgefüllt zu werden. Die folgenden Erläuterungen werden Ihnen dabei behilflich sein, alle notwendigen Felder auszufüllen.

Aktiv	Markieren Sie dieses Kästchen, um diese Funktion zu aktivieren.



Max. Leerlaufzeit - Wenn die Verbindung des externen Benutzers länger als die maximale Leerlaufzeit keine Aktivität aufweist, bricht der Router die Verbindung ab. Standardmäßig beträgt die maximale Leerlaufzeit 300 Sekunden.

ISDN - Externen Benutzern erlauben, sich über ISDN einzuwählen. Außerdem können Sie unten die Rückrufeinstellungen konfigurieren. Richten Sie den Benutzernamen und das Passwort des externen Benutzers unten ein.

PPTP - Dem externen Benutzer erlauben, über das Internet eine PPTP VPN-Verbindung aufzubauen. Richten Sie den Benutzernamen und das Passwort des externen Benutzers unten ein.

IPSec-Tunnel - Dem externen Benutzer erlauben, über das Internet eine IPSec VPN-Verbindung aufzubauen.

L2TP - Dem externen Benutzer erlauben, über das Internet eine L2TP VPN-Verbindung aufzubauen. Sie können L2TP entweder alleine oder zusammen mit IPSec wählen. Treffen Sie die Auswahl wie folgt:

Ohne - IPSec Policy nicht anwenden. Die VPN-Verbindung über L2TP ohne IPSec kann daher als reine L2TP-Verbindung betrachtet werden.

Falls vorhanden - Die IPSec Policy wird nur angewendet falls sie beim Verbindungsaufbau vorhanden ist. Ansonsten wird die Einwahl-VPN-Verbindung eine reine L2TP-Verbindung.

Erforderlich - Geben Sie die IPSec Policy an, die auf jeden Fall für die L2TP-Verbindung erforderlich ist.

Fernzugriff definieren - Wenn Sie das Kästchen markieren, können Sie die IP-Adresse des externen Benutzers, die ISDN-Nummer oder die Peer-ID angeben (kommt im IKE Aggressive Mode zur Anwendung).

Falls Sie das Kästchen abwählen, wendet der oben gewählte Verbindungstyp die Authentifizierungsmethoden und Sicherheitsmethoden der **Basiskonfiguration** an.

NetBIOS-Name durchlassenDurchlassen – Anklicken, damit bei der Verbindung zwischen den Hosts an beiden Enden des VPN-Tunnels der NetBIOS-Name durchgelassen wird.

Blockieren – Falls bei der Verbindung zwischen den Hosts an beiden Enden des VPN-Tunnels ein Konflikt auftritt, kann diese Funktion die Übertragung von NetBIOS-Namen im Tunnel blockiert werden.

Benutzername - Dieses Feld wird benötigt, wenn Sie oben ISDN, PPTP oder L2TP mit oder ohne IPSec wählen.

Passwort - Dieses Feld wird benötigt, wenn Sie oben ISDN, PPTP oder L2TP mit oder ohne IPSec wählen.

IKE-Authentifizierungsmethode - Diese Felder werden für IPSec-Tunnel und L2TP mit IPSec verwendet, wenn Sie die IP-Adresse des entfernten Knoten angeben. Die einzige Ausnahme ist die digitale Signatur (X.509), welche bei Auswahl des IPSec-Tunnels unter Angabe oder ohne Angabe der IP-Adresse des entfernten Knoten gesetzt werden kann.

Pre-Shared Key - Markieren Sie das Kästchen für den Pre-Shared Key, um diese Funktion zu aktivieren, und geben Sie die erforderlichen Zeichen (1-63) als Pre-Shared Key ein.

Digitale Signatur (X.509) – Markieren Sie das Kästchen für digitale Signatur, um diese Funktion zu aktivieren, und wählen Sie eines der vordefinierten Profile, das unter **VPN**

und externe Einwahl >>IPSec-Identität eingerichtet wurde.

IPSec-Sicherheitsmethode - Diese Felder sind für IPSec-Tunnel und L2TP mit IPSec notwendig, wenn Sie den entfernten Knoten angeben. Markieren Sie die Kästchen für das Medium, DES, 3DES oder AES als Sicherheitsmethode.

MittelAuthentication Header (AH) - bedeutet, dass die Daten authentifiziert, jedoch nicht verschlüsselt werden. Diese Option ist standardmäßig angehakt. Sie können die Option deaktivieren, indem Sie das Häkchen entfernen.

Hoch - Encapsulating Security Payload (ESP) - bedeutet, dass die Nutzdaten sowohl verschlüsselt als auch authentifiziert werden. Als Verschlüsselungsalgorithmus stehen DES (Data Encryption Standard), 3DES (Triple DES) und AES zur Verfügung.

Lokale ID - Geben Sie eine lokale ID an, die für die Einwahleinstellungen im LAN-zu-LAN-Profil zu verwenden ist. Dieser Punkt ist optional und kommt nur im IKE Aggressive Mode zur Anwendung.

Rückrufeinstellungen - Die Rückruffunktion ermöglicht nur für den externen ISDN-Benutzer einen Rückrufdienst. Der externe Benutzer zahlt die Verbindungsgebühren seines Anbieters.

Rückruffunktion aktiv - Aktiviert die Rückruffunktion.

Rückrufnummer festlegen - Diese Option bietet zusätzliche Sicherheit. Bei Aktivierung ruft der Router NUR die angegebene Rückrufnummer an.

Rückrufzeitkonto aktiv - Die Rückruffunktion unterliegt standardmäßig einer Zeitbeschränkung. Sobald das Rückrufkonto leer ist, wird der Rückrufmechanismus automatisch deaktiviert.

Max. Rückrufdauer (Einheit: Minuten) - Geben Sie das für den externen Benutzer verfügbare Zeitguthaben ein. Das Zeitguthaben verringert sich automatisch bei jeder Rückrufverbindung.

5.9.6 LAN zu LAN

Hier können Sie LAN-zu-LAN-Verbindungen verwalten, indem Sie eine Tabelle verschiedener Verbindungsprofile unterhalten. Sie können Parameter wie die Verbindungsrichtung (Einwahl oder Anwahl), die Peer-ID, Verbindungstyp (VPN-Verbindung einschl. PPTP, IPSec Tunnel und L2TP mit oder ohne IPSec), Sicherheitsmethoden usw. einstellen.

Der Router unterstützt bis zu 32 VPN-Tunnel. Die folgende Abbildung zeigt die Profilübersicht.

VPN und externe Einwahl >> LAN-zu-LAN

LAN-zu-LAN Profile: | Auf Werkseinstellungen zurücksetzen |

Index	Name	Status	Index	Name	Status
1.	???	X	17.	???	X
2.	???	X	18.	???	X
3.	???	X	19.	???	X
4.	???	X	20.	???	X
5.	???	X	21.	???	X
6.	???	X	22.	???	X
7.	???	X	23.	???	X
8.	???	X	24.	???	X
9.	???	X	25.	???	X
10.	???	X	26.	???	X
11.	???	X	27.	???	X
12.	???	X	28.	???	X
13.	???	X	29.	???	X
14.	???	X	30.	???	X
15.	???	X	31.	???	X
16.	???	X	32.	???	X

Auf Werkseinstellungen zurücksetzen - Klicken Sie auf diese Taste, um alle Einträge zu löschen.

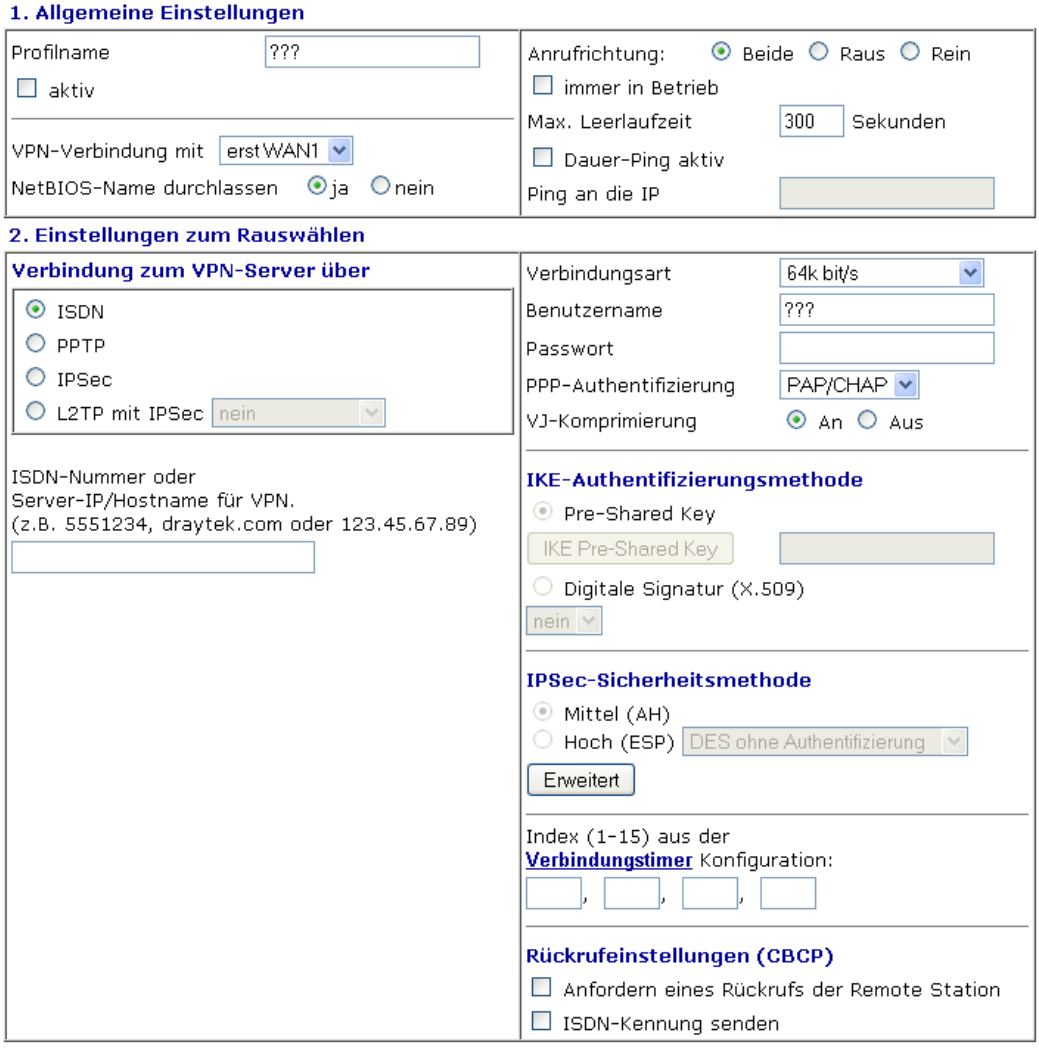
Name - Geben Sie den Namen des LAN-zu-LAN-Profils ein. Die Zeichen **???** lassen erkennen, dass das Profil leer ist.

Status - Zeigt den Status einzelner Profile an. "V" zeigt an, dass das Profil aktiv ist, während "X" anzeigt, dass es inaktiv ist.

Klicken Sie auf eine der Indexnummern, um das entsprechende Profil zu bearbeiten und auf die folgende Seite zu gelangen. Jedes LAN-zu-LAN-Profil beinhaltet vier Untergruppen. Ausgegraute Felder brauchen nicht ausgefüllt zu werden. Die folgenden Erläuterungen werden Ihnen dabei behilflich sein, alle notwendigen Felder auszufüllen.

Da der Dialog sehr umfangreich ist, sind die Erläuterungen in mehrere Abschnitte aufgeteilt.

VPN und externe Einwahl >> LAN-zu-LAN



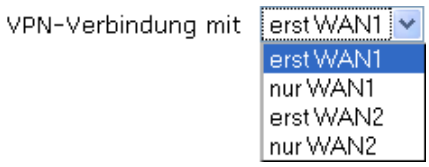
Profilname - Geben Sie einen Namen für das LAN-zu-LAN-Verbindungsprofil an.

Aktiv - Dieses Kästchen markieren, um das Profil zu aktivieren.

NetBIOS-Name durchlassen – Anklicken, damit bei der Verbindung zwischen den Hosts an beiden Enden des VPN-Tunnels der NetBIOS-Name durchgelassen wird.

Blockieren – Falls bei der Verbindung zwischen den Hosts an beiden Enden des VPN-Tunnels ein Konflikt auftritt, kann diese Funktion die Übertragung von NetBIOS-Namen im Tunnel blockiert werden.

VPN-Verbindung mit - Verwenden Sie das Dropdown-Menü, um die richtige WAN-Schnittstelle für diese Profil zu wählen. Diese Einstellung ist nur für die Anwahl nützlich.



Erst WAN1 - Der Router verwendet WAN1 als ersten Kanal für die VPN-Verbindung. Falls WAN1 nicht funktioniert, verwendet der Router stattdessen eine andere WAN-Schnittstelle.

Nur WAN1 - Der Router verwendet WAN1 als einzigen Kanal für die VPN-Verbindung.

Erst WAN2 - Der Router verwendet WAN2 als ersten Kanal für die VPN-Verbindung. Falls WAN2 nicht funktioniert, verwendet der Router stattdessen eine andere WAN-Schnittstelle.

Nur WAN2 - Der Router verwendet WAN2 als einzigen Kanal für die VPN-Verbindung.

Anrufrichtung - Angabe der zulässigen Anrufrichtung dieses LAN-zu-LAN-Profils.

Beide - Anwahl/Einwahl

Raus - nur Anwahl

Rein - nur Einwahl

Immer in Betrieb oder Max. LeerlaufzeitImmer in Betrieb - Markieren Sie diesen Punkt, damit der Router die VPN-Verbindung ständig aufrecht erhält.

Max. Leerlaufzeit: - Der Standardwert beträgt 300 Sekunden. Wird die Verbindung für einen längeren Zeitraum nicht genutzt, so bricht der Router die Verbindung ab.

Dauer-Ping aktiv - Diese Funktion ermöglicht dem Router, den Status der IPSec VPN-Verbindung zu erkennen und ist besonders im Falle von anormalen Unterbrechungen des VPN IPSec-Tunnels hilfreich. Einzelheiten werden unten erläutert. Markieren Sie dieses Kästchen, um die Übertragung von Ping-Paketen an die angegebene IP-Adresse zu ermöglichen.

Ping an die IP - Geben Sie die IP-Adresse des entfernten Hosts an, der sich am anderen Ende des VPN-Tunnels befindet.

Dauer-Ping aktiv wird für anormale Unterbrechungen von IPSec VPN-Verbindungen verwendet. Auf diese Weise kann der Status einer VPN-Verbindung ermittelt werden, aufgrund dessen der Router erkennt, ob eine Wiederwahl erforderlich ist.

Wenn einer der VPN-Peers die Verbindung

beenden möchte, sollten normalerweise zur gegenseitigen Information eine Reihe von Paketen ausgetauscht werden. Falls der entfernte Peer jedoch ohne vorherige Benachrichtigung abbrechen sollte, kann der Vigor-Router dies nicht wissen. Um dieses Problem zu lösen, kann der Vigor-Router ständig Ping-Pakete an den entfernten Router senden, um über den Status der VPN-Verbindung informiert zu sein und entsprechend zu reagieren. Dies geschieht unabhängig von DPD (Dead Peer Detection).

PPTP - PPTP VPN-Verbindung zum Server über das Internet aufbauen. Richten Sie für die Authentifizierung des entfernten Servers unten eine Identität mit Benutzernamen und Passwort ein.

IPSec-Tunnel - IPSec VPN-Verbindung zum Server über das Internet aufbauen.

L2TP mit … - L2TP VPN-Verbindung über das Internet aufbauen. Sie können L2TP entweder alleine oder zusammen mit IPSec wählen. Treffen Sie die Auswahl wie folgt:

Ohne: - IPSec Policy nicht anwenden. Die VPN-Verbindung über L2TP ohne IPSec kann daher als reine L2TP-Verbindung betrachtet werden.

Falls vorhanden: - Die IPSec Policy wird nur angewendet falls sie beim Verbindungsaufbau vorhanden ist. Ansonsten wird die Anwahl-VPN-Verbindung eine reine L2TP-Verbindung.

Erforderlich: - Geben Sie die IPSec Policy an, die auf jeden Fall für die L2TP-Verbindung erforderlich ist.

Benutzername - Dieses Feld wird benötigt, wenn Sie oben ISDN, PPTP oder L2TP mit oder ohne IPSec wählen.

Passwort - Dieses Feld wird benötigt, wenn Sie oben ISDN, PPTP oder L2TP mit oder ohne IPSec wählen.

PPP-Authentifizierung - Dieses Feld wird benötigt, wenn Sie oben ISDN, PPTP oder L2TP mit oder ohne IPSec wählen. Wegen der breiten Kompatibilität ist PAP/CHAP die üblichste Auswahl.

VJ-Komprimierung - Dieses Feld wird benötigt, wenn Sie oben ISDN, PPTP oder L2TP mit oder ohne IPSec wählen. VJ-Komprimierung wird für TCP/IP-Protokoll-

Header-Komprimierung verwendet. Setzen Sie diese Option auf **Ja**, um die Bandbreite bestmöglich auszunutzen.

IKE-Authentifizierungsmethode - Diese Felder sind für IPSec-Tunnel und L2TP mit IPSec bestimmt.

Pre-Shared Key - Eingabe von 1-63 Zeichen als Pre-Shared Key.

Digitale Signatur (X.509) - Wählen Sie eines der vordefinierten Profile, das unter **VPN und externe Einwahl >>IPSec-Identität** eingerichtet wurde.

IPSec-Sicherheitsmethode - Diese Felder sind für IPSec-Tunnel und L2TP mit IPSec erforderlich.

MittelAuthentication Header (AH) - bedeutet, dass die Daten authentifiziert, jedoch nicht verschlüsselt werden. Diese Option ist standardmäßig aktiviert.

Hoch (ESP - Encapsulating Security Payload) - bedeutet, dass die Nutzdaten sowohl verschlüsselt als auch authentifiziert werden. Treffen Sie die Auswahl wie folgt:

DES ohne Authentifizierung - DES-Verschlüsselungsalgorithmus ohne jegliche Authentifizierung verwenden.

DES mit Authentifizierung - DES-Verschlüsselungsalgorithmus mit Authentifizierungsalgorithmus MD5 oder SHA-1 verwenden.

3DES ohne Authentifizierung - 3DES-Verschlüsselungsalgorithmus ohne jegliche Authentifizierung verwenden.

3DES mit Authentifizierung - 3DES-Verschlüsselungsalgorithmus mit Authentifizierungsalgorithmus MD5 oder SHA-1 verwenden.

AES ohne Authentifizierung - AES-Verschlüsselungsalgorithmus ohne jegliche Authentifizierung verwenden.

AES mit Authentifizierung - AES-Verschlüsselungsalgorithmus mit Authentifizierungsalgorithmus MD5 oder SHA-1 verwenden.

Erweitert - Ermöglicht die Angabe von Modus, Proposal und Gültigkeitsdauer des Schlüssels jeder IKE-Phase, Gateway, usw.

Das Fenster der erweiterten Konfiguration sieht wie folgt aus:

IKE Phase 1 Modus - Sie haben die Wahl zwischen **Main** und **Aggressive**. Der Zweck besteht im Austausch von Verschlüsselungsvorschlägen zur Einrichtung eines geschützten, sicheren Kanals. Der **Main**-Modus ist sicherer als der **Aggressive**-Modus, da ein größerer Teil des Austauschs zur Einrichtung der IPSec-Sitzung über einen sicheren Kanal stattfindet. Der **Aggressive**-Modus ist jedoch schneller. Standardmäßig verwendet der Vigor-Router den Main-Modus.

IKE Phase 1 Proposal - Wird verwendet, um den VPN-Peers die lokal verfügbaren Authentifizierungsmethoden und Verschlüsselungsalgorithmen vorzuschlagen und diesbezüglich eine Rückmeldung zu erhalten. Es sind zwei Kombinationen für den **Aggressive**-Modus und neun für den **Main**-Modus verfügbar. Wir empfehlen die Auswahl der Kombination, welche die meisten Methoden abdeckt.

IKE Phase 2 Proposal - Wird verwendet, um den VPN-Peers die lokal verfügbaren Algorithmen vorzuschlagen und diesbezüglich eine Rückmeldung zu erhalten. Für beide Modi sind drei Kombinationen verfügbar. Wir empfehlen die Auswahl der Kombination, welche die meisten Algorithmen abdeckt.

IKE Phase 1 Key Lifetime - Aus Sicherheitsgründen sollte die Gültigkeitsdauer des Schlüssels definiert werden. Der Standardwert beträgt 28800 Sekunden. Sie können einen Wert zwischen 900 und 86400 Sekunden eingeben.

IKE Phase 2 Key Lifetime - Aus Sicherheitsgründen sollte die Gültigkeitsdauer des Schlüssels definiert werden. Der Standardwert beträgt 3600 Sekunden. Sie können einen Wert zwischen 600 und 86400 Sekunden eingeben.

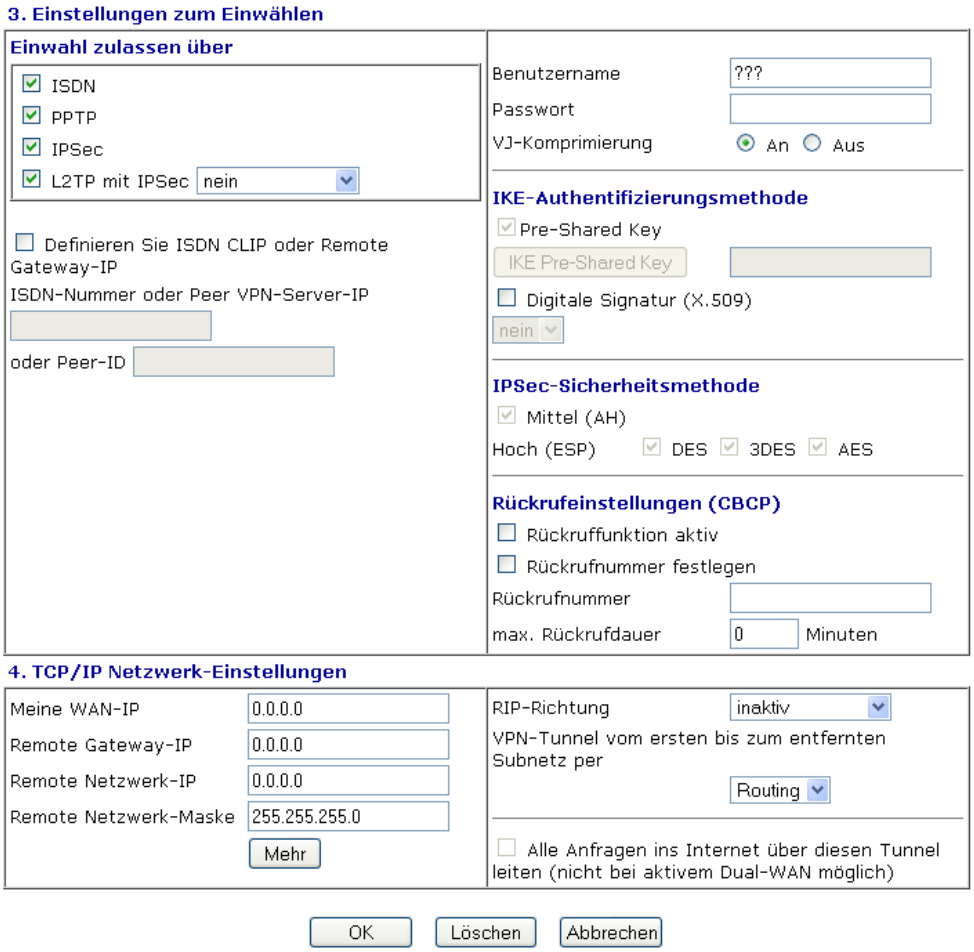
Perfect Forward Secret (PFS) - Der IKE Phase 1 Schlüssel wird wiederverwendet, um den komplexen Rechenvorgang in Phase 2 zu vermeiden. Der Standardwert dieser Funktion ist inaktiv.

Lokale ID - Im **Aggressive** Mode steht bei der Authentifizierung gegen den entfernten VPN-Server die lokale ID für die IP-Adresse. Die Länge der ID ist auf 47 Zeichen beschränkt.

Rückrufeinstellungen - Die Rückruffunktion ermöglicht im Rahmen der PPP-Suite nur für den externen ISDN-Benutzer einen Rückrufdienst. Der Besitzers des Routers zahlt die Verbindungsgebühren seines Anbieters.

Anfordern eines Rückrufs der Remote Station - Aktivieren Sie diese Option, damit der Router für die folgende Verbindung einen Rückruf der entfernten Station anfordert.

ISDN-Kennung senden - Falls die entfernte Station vom Vigor-Router einen Rückruf anfordert, wird die lokale ISDN-Nummer an die entfernte Station gesendet. Markieren Sie dieses Kästchen, um dem Vigor-Router zu erlauben, die ISDN-Nummer an die entfernte Station zu senden.



Einwahl zulassen über - Bestimmen Sie, wie die Einwahl stattfinden darf.

ISDN - Erlaubt eine entfernte ISDN LAN-zu-LAN-Verbindung. Richten Sie den Benutzernamen und das Passwort des externen Benutzers unten ein. Außerdem können Sie unten die Rückrufeinstellungen konfigurieren.

PPTP - Dem externen Benutzer erlauben, über das Internet eine PPTP VPN-Verbindung aufzubauen. Richten Sie den Benutzernamen und das Passwort des externen Benutzers unten ein.

IPSec-Tunnel - Dem externen Benutzer erlauben, über das Internet eine IPSec VPN-Verbindung anzustoßen.

L2TP - Dem externen Benutzer erlauben, über das Internet eine L2TP VPN-Verbindung aufzubauen. Sie können L2TP entweder alleine oder zusammen mit IPSec wählen. Treffen Sie die Auswahl wie folgt:

Ohne - IPSec Policy nicht anwenden. Die VPN-Verbindung über L2TP ohne IPSec kann daher als reine L2TP-Verbindung betrachtet werden.

Falls vorhanden - Die IPSec Policy wird nur angewendet falls sie beim Verbindungsaufbau vorhanden ist. Ansonsten wird die Einwahl-VPN-Verbindung eine reine L2TP-Verbindung.

Erforderlich - Geben Sie die IPSec Policy an, die auf jeden Fall für die L2TP-Verbindung erforderlich ist.

CLIP oder entferntes ISDN Gateway - Markieren Sie das Kästchen, um die IP-Adresse des externen Benutzers oder die Peer-ID (sollte der ID entsprechen, die unter "Einwahl zulassen über" eingegeben wurde. Geben Sie die Peer ISDN-Nummer ein, falls Sie oben ISDN gewählt haben. Bestimmen Sie außerdem die entsprechenden Sicherheitsmethoden auf der rechten Seite.

Falls Sie das Kästchen abwählen, wendet der oben gewählte Verbindungstyp die Authentifizierungsmethoden und Sicherheitsmethoden der Basiskonfiguration an.

Benutzername - Dieses Feld wird benötigt, wenn Sie oben ISDN, PPTP oder L2TP mit oder ohne IPSec wählen.

Passwort - Dieses Feld wird benötigt, wenn Sie oben ISDN, PPTP oder L2TP mit oder ohne IPSec wählen.

VJ-Komprimierung - VJ-Komprimierung wird für TCP/IP-Protokoll-Header-Komprimierung verwendet. Dieses Feld wird benötigt, wenn Sie oben ISDN, PPTP oder L2TP mit oder ohne IPSec wählen.

IKE-Authentifizierungsmethode - Diese Felder werden für IPSec-Tunnel und L2TP mit IPSec verwendet, wenn Sie die IP-Adresse des entfernten Knoten angeben. Die einzige Ausnahme ist die digitale Signatur (X.509), welche bei Auswahl des IPSec-Tunnels unter Angabe oder ohne Angabe der IP-Adresse des entfernten Knoten gesetzt werden kann.

Pre-Shared Key - Markieren Sie das Kästchen für den Pre-Shared Key, um diese Funktion zu aktivieren, und geben Sie die erforderlichen Zeichen (1-63) als Pre-Shared Key ein.

Digitale Signatur (X.509) – Markieren Sie das

Kästchen für digitale Signatur, um diese Funktion zu aktivieren, und wählen Sie eines der vordefinierten Profile, das unter **VPN und externe Einwahl >>IPSec-Identität** eingerichtet wurde.

IPSec-Sicherheitsmethode - Diese Felder sind für IPSec-Tunnel und L2TP mit IPSec notwendig, wenn Sie den entfernten Knoten angeben.

Mittel - Authentication Header (AH) bedeutet, dass die Daten authentifiziert, jedoch nicht verschlüsselt werden. Diese Option ist standardmäßig aktiviert.

Hoch - Encapsulating Security Payload (ESP) bedeutet, dass die Nutzdaten sowohl verschlüsselt als auch authentifiziert werden. Als Verschlüsselungsalgorithmus stehen DES (Data Encryption Standard), 3DES (Triple DES) und AES zur Verfügung.

Rückrufeinstellungen - Die Rückruffunktion ermöglicht nur für die ISDN LAN-zu-LAN-Verbindung einen Rückrufdienst. Der externe Benutzer zahlt die Verbindungsgebühren seines Anbieters.

Rückruffunktion aktiv - Aktiviert die Rückruffunktion.

Rückrufnummer - Diese Option bietet zusätzliche Sicherheit. Bei Aktivierung ruft der Router NUR die angegebene Rückrufnummer an.

Max. Rückrufdauer - Die Rückruffunktion ist standardmäßig zeitlich begrenzt. Sobald das Rückrufkonto leer ist, wird die Funktion automatisch deaktiviert.

Max. Rückrufdauer (Einheit: Minuten) - Geben Sie das für den externen Benutzer verfügbare Zeitguthaben ein. Das Zeitguthaben verringert sich automatisch bei jeder Rückrufverbindung. Der Standardwert 0 bedeutet, dass die Rückrufdauer unbegrenzt ist.

Meine WAN-IP - Dieses Feld wird nur benötigt, wenn Sie oben ISDN, PPTP oder L2TP mit oder ohne IPSec wählen. Der Standardwert ist 0.0.0.0, was bedeutet, dass der Vigor-Router während der IPCP-Verhandlungsphase eine PPP IP-Adresse vom entfernten Router erhält. Falls die PPP IP von der entfernten Seite festgelegt wird, geben Sie hier die feste IP-Adresse ein. Ändern Sie den Standardwert nur, falls Sie ISDN, PPTP oder L2TP verwenden.

Remote Gateway-IP - Dieses Feld wird nur benötigt, wenn Sie oben ISDN, PPTP oder

L2TP mit oder ohne IPSec wählen. Der Standardwert ist 0.0.0.0, was bedeutet, dass der Vigor-Router während der IPCP-Verhandlungsphase eine entfernte Gateway PPP IP-Adresse vom entfernten Router erhält. Falls die PPP IP von der entfernten Seite festgelegt wird, geben Sie hier die feste IP-Adresse ein. Ändern Sie den Standardwert nur, falls Sie ISDN, PPTP oder L2TP verwenden.

Remote Netzwerk-IP/ Remote Netzwerk-Maske - Fügen Sie eine statische Route hinzu, um den gesamten Verkehr, der an diese Remote Netzwerk-IP/Remote Netzwerk-Maske gerichtet ist, durch die VPN-Verbindung zu leiten. Bei IPSec ist dies die Ziel-Client-ID von Phase 2 Quick Mode.

Mehr - Fügen Sie eine statische Route hinzu, um den gesamten Verkehr, der an weitere Remote Netzwerk-IPs/Remote Netzwerk-Masken gerichtet ist, durch die VPN-Verbindung zu leiten. Dies trifft normalerweise zu, wenn sich hinter dem entfernten VPN-Router mehrere Subnetze befinden.

RIP-Richtung - Diese Option bestimmt die Richtung der RIP-Pakete (Routing Information Protocol). Sie können hier Richtungen aktivieren/deaktivieren. Es stehen vier Optionen zur Auswahl: Beide (TX/RX), Nur TX, Nur RX und Inaktiv.

Vom ersten bis zum entfernten Subnetz soll der VPN-Tunnel - Falls das entfernte Netzwerk lediglich die Einwahl mit einer einzigen IP erlaubt, wählen Sie **NAT**, ansonsten **Route**.

Alle Anfragen ins Internet über diesen Tunnel leiten - Markieren Sie dieses Kästchen, um diesen VPN-Tunnel als Standard-Route zu bestimmen. Bitte beachten Sie, dass diese Option lediglich verfügbar ist, wenn eine WAN-Schnittstelle aktiviert ist. Sie ist nicht verfügbar, wenn beide WAN-Schnittstellen aktiviert sind. Um diese Einstellung zu nutzen, müssen Sie eine WAN-Schnittstelle (WAN 1 oder WAN 2) unter **WAN >> Basiskonfiguration** deaktivieren.

5.9.7 Verbindungsmanagement

Hier finden Sie eine tabellarische Zusammenfassung aller VPN-Verbindungen. Sie können jede beliebige VPN-Verbindung durch Klicken auf **Trennen** beenden. Aggressive Anwahl ist mit Hilfe des Anwahl-Tools und Klicken auf **Wählen** möglich.

Wählen - Klicken Sie auf diese Taste, um die Anwahlfunktion auszuführen.

Aktualisierungsintervall - Wählen Sie die Zeit für die Aktualisierung der Wählinformationen (5, 10 oder 30 Sekunden).

Aktualisieren - Klicken Sie auf diese Taste, um den gesamten Verbindungsstatus zu aktualisieren.

5.10 Zertifikatsverwaltung

Ein digitales Zertifikat dient als elektronischer Ausweis und wird von einer Zertifizierungsstelle (Certification Authority - CA) ausgegeben. Es enthält Informationen wie Ihren Namen, eine laufende Nummer, Verfallsdatum usw. sowie die digitale Signatur der ausgebenden Stelle, so dass ein Empfänger die Echtheit des Zertifikats verifizieren kann. Der Vigor-Router unterstützt digitale Zertifikate gemäß dem Standard X.509.

Zur Verwendung von digitalen Zertifikaten sollte zunächst ein von einem CA-Server ausgegebenes Zertifikat angefordert werden. Die Zertifikate anderer vertrauenswürdiger CA-Server sollten auch heruntergeladen werden, um die Gegenstelle mit den von diesen vertrauenswürdigen CA-Servern ausgegebenen Zertifikaten authentifizieren zu können.

Hier können Sie lokale digitale Zertifikate generieren und verwalten und vertrauenswürdige CA-Zertifikate setzen. Achten Sie darauf, dass die Uhrzeit des Vigor-Routers korrekt eingestellt ist, bevor Sie das Zertifikat verwenden, damit die Gültigkeitsdauer des Zertifikats korrekt ist.

Die folgende Abbildung zeigt die Menüeinträge für die Zertifikatsverwaltung:

5.10.1 Lokales Zertifikat

Erstellen - Klicken Sie auf diese Taste, um das Fenster **Zertifikat erstellen** zu öffnen.

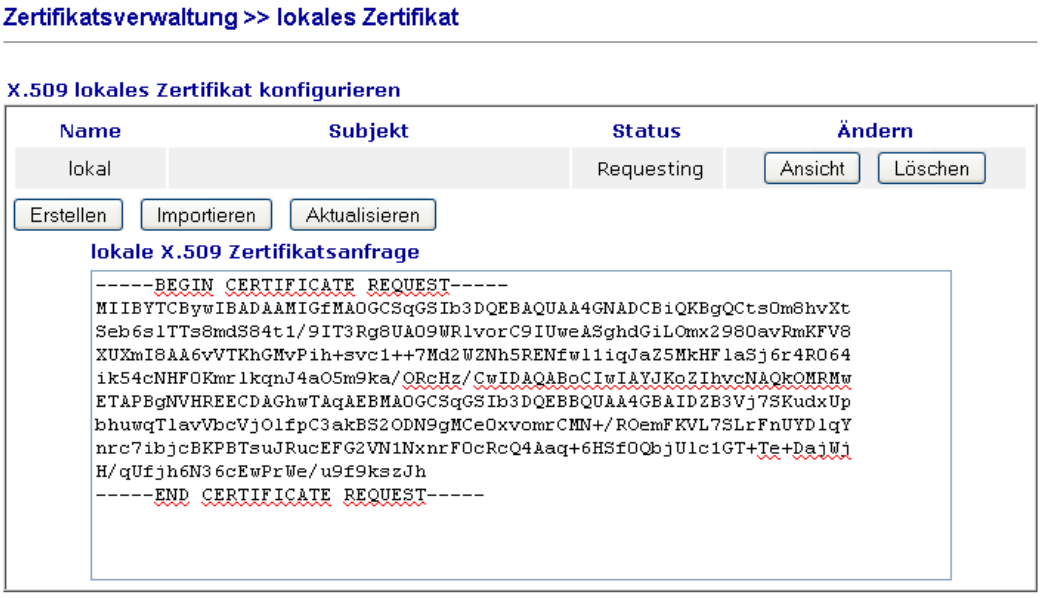
Geben Sie alle Daten ein, die das Fenster anfordert. Dann klicken Sie erneut auf **Erstellen**.

Import - Klicken Sie auf diese Taste, um eine gespeicherte Datei mit Zertifizierungsinformationen zu importieren.

Aktualisieren - Klicken Sie auf diese Taste, um die unten aufgeführte Information zu aktualisieren.

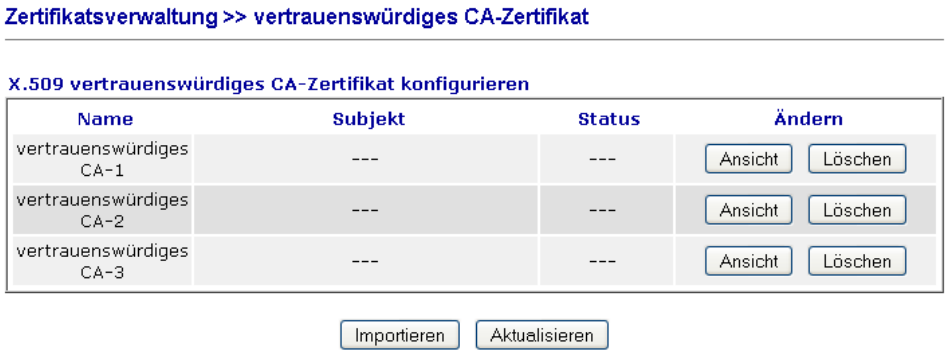
Ansicht - Klicken Sie auf diese Taste, um die Detaileinstellungen für die Erstellung eines Zertifikats zu sehen.

Nachdem Sie **Erstellen** angeklickt haben, wird die erzeugte Information im Fenster unten angezeigt:

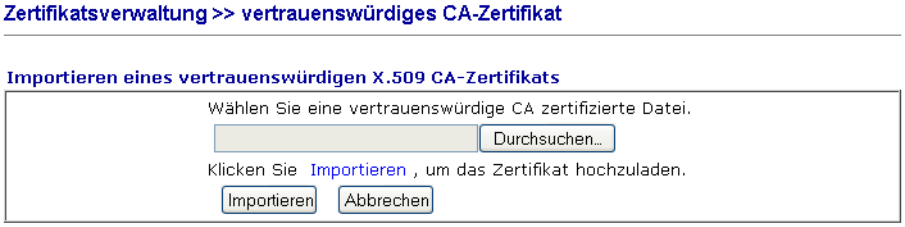


5.10.2 Vertrauenswürdiges CA-Zertifikat

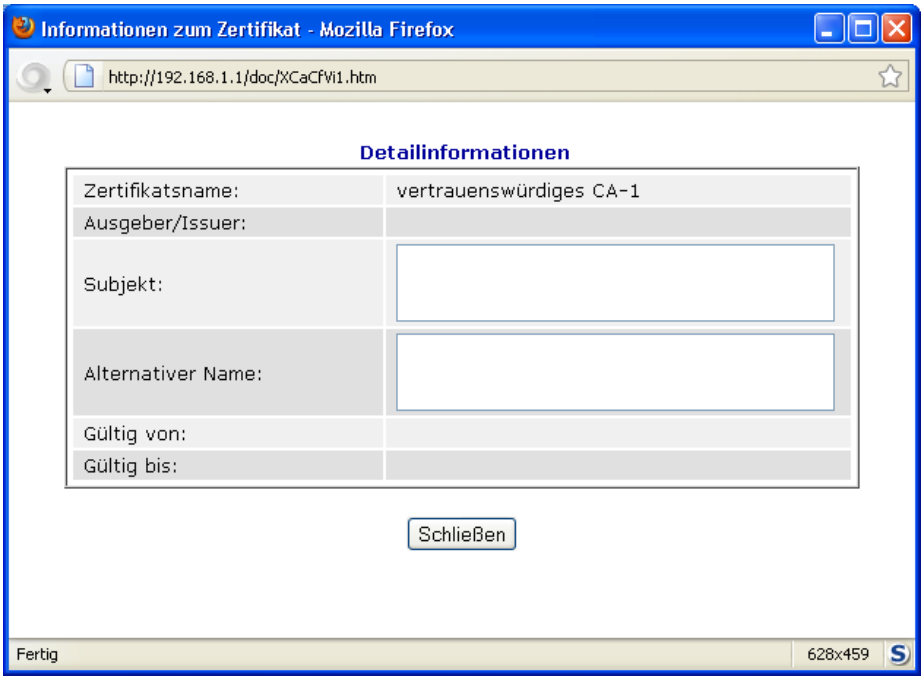
Unter diesem Punkt werden drei vertrauenswürdige CA-Zertifikate aufgeführt.



Um ein zuvor gespeichertes vertrauenswürdiges CA-Zertifikat zu importieren, klicken Sie bitte auf **Importieren**, wodurch sich das folgende Fenster öffnet. Verwenden Sie **Durchsuchen…**, um die gespeicherte Textdatei zu finden. Dann klicken Sie auf **Importieren**. Das importierte Zertifikat wird im Fenster für vertrauenswürdige CA-Zertifikate aufgeführt.



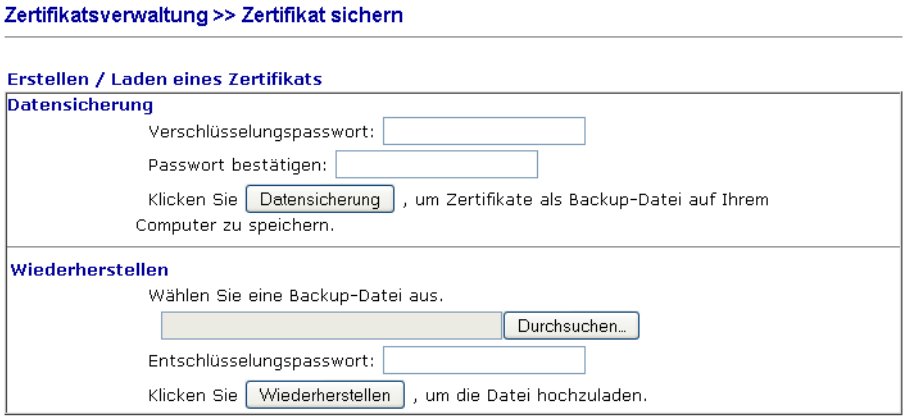
Sie können die einzelnen vertrauenswürdigen CA-Zertifikate betrachten, indem Sie das detaillierte Infofenster durch Klicken auf **Ansicht** öffnen. Um ein CA-Zertifikat zu löschen, markieren Sie es und klicken auf **Löschen**, wodurch alle Zertifikatsinformationen gelöscht werden.



5.10.3 Zertifikat sichern

Das lokale Zertifikat und das vertrauenswürdige CA-Zertifikat für diesen Router können in einer Datei gespeichert werden. Klicken Sie im folgenden Dialog auf **Backup**, um die Zertifikate zu speichern. Falls Sie ein Verschlüsselungspasswort für diese Zertifikate setzen möchten, geben Sie bitte die entsprechenden Zeichenfolgen in **Verschlüsselungspasswort** und **Passwort bestätigen** ein.

Sie können jederzeit **Wiederherstellen** verwenden, um diese beiden Einstellungen auf dem Router wiederherzustellen.

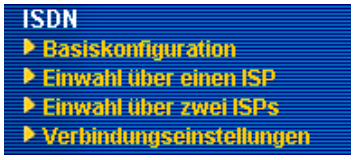


5.11 ISDN

5.11.1 Grundkonzept

ISDN (Abkürzung für "Integrated Services Digital Network") ist ein internationaler Kommunikationsstandard für die Übertragung von Sprache, Video und Daten über digitale oder analoge Telefonleitungen.

Die folgende Abbildung zeigt die Menüeinträge für ISDN:



5.11.2 Basiskonfiguration

Auf dieser Seite können Sie grundlegende ISDN-Einstellungen wie die Aktivierung des ISDN-Ports, MSN-Nummern, blockierte MSN-Nummern usw. vornehmen.

ISDN-Port - Klicken Sie auf **Aktiv**, um den ISDN-Port zu öffnen, oder auf **Inaktiv**, um ihn zu schließen.

Land - Zum korrekten Betrieb mit ihrem örtlichen ISDN-Netz wählen Sie bitte das richtige Land.

D-Kanal Modus - Hier können Sie das ISDN Layer2 Protokoll wie folgt konfigurieren:

Point-to-Point - Mit dieser Option verwendet der ISDN-Port einen statischen TEI (Terminal Endpoint Identifier).

Point-to-Multipoint - Mit dieser Option verwendet der ISDN-Port einen dynamischen TEI.

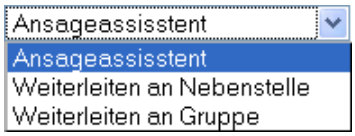
Eigene Nummer - Geben Sie Ihre ISDN-Nummer ein. Bei jedem ausgehenden Anruf wird die Nummer an den Empfänger übermittelt.

Blockierte MSN-Nummern für den Router - Geben Sie die entsprechende MSN-Nummer im Feld ein, um zu vermeiden, dass der Router diese MSN-Nummer anwählt.

MSN-Nummern für den Router - Werden **MSN-Nummern** eingerichtet, so nimmt der Router nur eingehende Anrufe an, deren Nummern übereinstimmen. MSN-Dienste

sollten vom örtlichen ISDN-Anbieter unterstützt werden. Der Router bietet drei Felder für MSN-Nummern. Beachten Sie, dass Sie die MSN-Dienste von Ihrem örtlichen Telekom-Anbieter beantragen müssen. Die MSN-Funktion ist standardmäßig deaktiviert. Falls Sie die Felder leer lassen, werden alle eingehenden Anrufe angenommen, ohne auf Übereinstimmung der Nummern zu achten.

Anrufbeantwortungsmodus - Geben Sie an, wie mit eingehenden Anrufen umgegangen werden soll, die der MSN-Nummer für den Router entsprechen.



Ansageassistent - Eingehende Anrufe werden automatisch vom Router angenommen. Die Ansage kann Sie dazu auffordern, die Nebenstelle zu wählen, die Sie erreichen möchten.

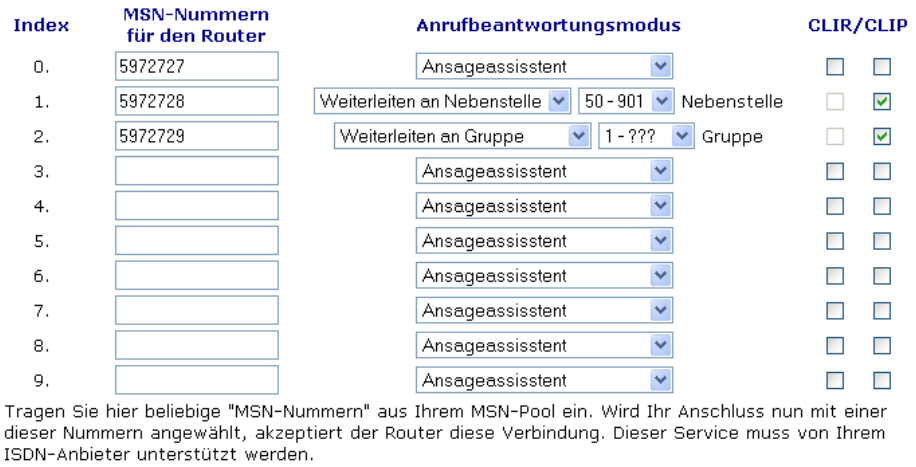
Weiterleiten an Nebenstelle - Eingehende Anrufe werden direkt an die konfigurierte Nebenstellenrufnummer weitergeleitet.

Weiterleiten an Gruppe - Falls Sie auf der entsprechenden Seite eine Nebenstellengruppe konfiguriert haben, können eingehende Anrufe an die ausgewählte Nebenstellengruppe weitergeleitet werden.

CLIR/CLIP - Markieren Sie dieses Kästchen, um die Übermittlung der Anrufer-ID an die Gegenstelle zu erlauben oder zu verbergen.

Beispiel:

Die folgende Abbildung zeigt, wie MSN-Nummern für den TE-Port aussehen können:



Index	MSN-Nummern für den Router	Anrufbeantwortungsmodus	CLIR/CLIP
0.	5972727	Ansageassisstent	☐ ☐
1.	5972728	Weiterleiten an Nebenstelle 50 - 901 Nebenstelle	☐ ☑
2.	5972729	Weiterleiten an Gruppe 1 - ??? Gruppe	☐ ☑
3.		Ansageassisstent	☐ ☐
4.		Ansageassisstent	☐ ☐
5.		Ansageassisstent	☐ ☐
6.		Ansageassisstent	☐ ☐
7.		Ansageassisstent	☐ ☐
8.		Ansageassisstent	☐ ☐
9.		Ansageassisstent	☐ ☐

Tragen Sie hier beliebige "MSN-Nummern" aus Ihrem MSN-Pool ein. Wird Ihr Anschluss nun mit einer dieser Nummern angewählt, akzeptiert der Router diese Verbindung. Dieser Service muss von Ihrem ISDN-Anbieter unterstützt werden.

Erläuterung:

a. Falls Sie die **MSN-Nummern für den Router** wie in der obigen Abbildung konfigurieren, nimmt der Router nur die MSN-Nummern **5972727 / 5972728 / 5972729** an.

b. Wird der Router unter **5972727** angewählt, so wird der Anruf automatisch angenommen. Die Ansage kann Sie dazu auffordern, die Nebenstelle zu wählen, die Sie erreichen möchten.

c. Wird der Router unter **5972728** angewählt, so wird der Anruf automatisch an die Nebenstelle 100 weitergeleitet.

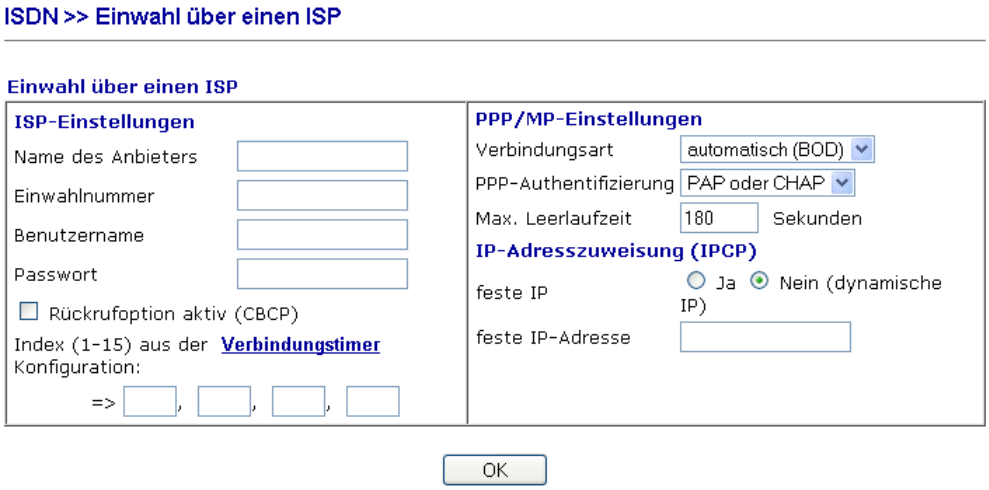
d. Wird der Router unter **5972729** angewählt, so wird der Anruf automatisch an die Gruppendurchwahl 300 weitergeleitet.

e. Wenn Sie ein Telefon mit der Nebenstellenrufnummer 100 verwenden, um einen ISDN-Anruf zu tätigen, so sieht das entfernte ISDN-Telefon die **Anrufer-ID 5972728** (sofern für das Telefon CLIP aktiviert ist).

f. Wenn Sie irgendeine der Nebenstellenrufnummern verwenden, die zur Gruppendurchwahl 300 gehört, um einen ISDN-Anruf zu tätigen, so sieht das entfernte ISDN-Telefon die **Anrufer-ID 5972729** (sofern für das Telefon CLIP aktiviert ist).

5.11.3 Einwahl über einen ISP

Wählen Sie **Einwahl über einen ISP**, falls Sie sich über einen einzelnen ISP im Internet einwählen.



ISP-EinstellungenName des Anbieters - Geben Sie den Namen Ihres ISPs ein.

Einwahlnummer - Geben Sie die von Ihrem ISP mitgeteilte ISDN-Einwahlnummer an.

Benutzername - Geben Sie den von Ihrem ISP mitgeteilten Benutzernamen ein.

Passwort - Geben Sie das von Ihrem ISP mitgeteilte Passwort ein.

Rückrufoption aktiv (CBCP) - Falls Ihr ISP die Rückruffunktion unterstützt, markieren Sie dieses Kästchen, um das Callback Control Protocol während der PPP-Aushandlung zu aktivieren.

Index (1-15) aus dem Verbindungstimer - Unter den Indexnummern gelangen Sie in die Timerprofile, mit denen Sie den Zugriff auf das Internet steuern können. Kapitel **5.8.2 Verbindungstimer** enthält Einzelheiten zur Konfiguration.

PPP/MP-EinstellungenVerbindungsart – Hier werden drei Verbindungsarten für verschiedene Zwecke angeboten. **Inaktiv** deaktiviert die ISDN-Anwahlfunktion. **64 kbit/s Leitung** erlaubt Ihnen die Nutzung eines ISDN B-Kanals zur Einwahl ins Internet. **128 kbit/s Leitung** ermöglicht Ihnen die Nutzung beider ISDN-Kanäle zur Einwahl ins Internet. **Automatisch (BOD)** ermöglicht die Nutzung der Bandbreite nach Bedarf (Einzelheiten zur Konfiguration werden in Kapitel **5.12.4** erläutert). Der Router benutzt bei niedrigem Verkehrsaufkommen lediglich einen B-Kanal. Sobald die Bandbreite des einzelnen B-Kanals verbraucht ist, wird der andere B-Kanal durch

die Anwahl automatisch aktiviert. Weitere Einzelheiten zu den BOD-Parametereinstellungen werden im Abschnitt unter **Verbindungseinstellungen** beschrieben.

PPP-Authentifizierung - Nur PAP - ermöglicht Ihnen, PPP-Sitzungen so zu konfigurieren, dass das PAP-Protokoll zur Verhandlung des Benutzernamens und Passworts mit dem ISP verwendet wird. **PAP oder CHAP** ermöglicht Ihnen, PPP-Sitzungen so zu konfigurieren, dass zur Verhandlung des Benutzernamens und Passworts mit dem ISP entweder das PAP-Protokoll oder das CHAP-Protokoll verwendet wird.

Max. Leerlaufzeit - Der Router wird nach der voreingestellten maximalen Leerlaufzeit getrennt. Die Standardeinstellung ist 180 Sekunden. Setzen Sie die Zeit auf 0, so wird die ISDN-Verbindung zum ISP dauerhaft aufrecht erhalten.

IP-Adresszuweisung (IPCP) - In den meisten Umgebungen ist es nicht nötig, diese Einstellungen zu ändern, da die meisten ISPs dem Router bei der Einwahl eine dynamische IP-Adresse zuweisen. Falls Ihnen Ihr ISP eine feste IP-Adresse zuweist, wählen Sie **Ja** und geben die IP-Adresse im Feld **Feste IP-Adresse** ein.

5.11.4 Einwahl über zwei ISPs

Wählen Sie **Einwahl über zwei ISPs**, falls Sie mehr als einen ISP haben. Sie können beide ISPs gleichzeitig anwählen. Dies ist hauptsächlich für ISPs, die ML-PPP (Multiple-Link PPP) nicht unterstützen. In solchen Fällen kann die Einwahl über zwei ISPs die verfügbare Bandbreite der ISDN-Kanäle auf 128 kbit/s erhöhen.

Allgemeine EinstellungenDuale ISP Funktion aktiv - Markieren Sie dieses Kästchen, um die Einwahl über zwei ISPs zu ermöglichen. **Rückrufoption aktiv (CBCP) -** Falls Ihr ISP die Rückruffunktion unterstützt, markieren Sie dieses Kästchen, um das Callback Control Protocol während der PPP-Aushandlung zu aktivieren.

PPP/MP-EinstellungenVerbindungsart – Hier werden drei Verbindungsarten für verschiedene Zwecke angeboten. **Inaktiv** deaktiviert die ISDN-Anwahlfunktion. **128 kbit/s Leitung** ermöglicht Ihnen die Nutzung beider ISDN-Kanäle zur Einwahl ins Internet. **Automatisch (BOD)** ermöglicht die Nutzung der Bandbreite nach Bedarf (Einzelheiten zur Konfiguration werden in Kapitel **5.12.4** erläutert). Der Router benutzt bei niedrigem Verkehrsaufkommen lediglich

einen B-Kanal. Sobald die Bandbreite des einzelnen B-Kanals verbraucht ist, wird der andere B-Kanal durch die Anwahl automatisch aktiviert.

PPP-Authentifizierung - Nur PAP ermöglicht Ihnen, PPP-Sitzungen so zu konfigurieren, dass das PAP-Protokoll zur Verhandlung des Benutzernamens und Passworts mit dem ISP verwendet wird. **PAP oder CHAP** ermöglicht Ihnen, PPP-Sitzungen so zu konfigurieren, dass zur Verhandlung des Benutzernamens und Passworts mit dem ISP entweder das PAP-Protokoll oder das CHAP-Protokoll verwendet wird.

Max. Leerlaufzeit - Der Router wird nach der voreingestellten maximalen Leerlaufzeit getrennt. Die Standardeinstellung ist 180 Sekunden. Setzen Sie die Zeit auf 0, so wird die ISDN-Verbindung zum ISP dauerhaft aufrecht erhalten.

Primäre ISP-EinstellungenName des Anbieters - Geben Sie den Namen Ihres ISPs ein.

Einwahlnummer - Geben Sie die von Ihrem ISP mitgeteilte ISDN-Einwahlnummer an.

Benutzername - Geben Sie den von Ihrem ISP mitgeteilten Benutzernamen ein.

Passwort - Geben Sie das von Ihrem ISP mitgeteilte Passwort ein.

IP-Adresszuweisung (IPCP) durch den ersten ISP - In den meisten Umgebungen ist es nicht nötig, diese Einstellungen zu ändern, da die meisten ISPs dem Router bei der Einwahl eine dynamische IP-Adresse zuweisen. Falls Ihnen Ihr ISP eine feste IP-Adresse zuweist, wählen Sie **Ja** und geben die IP-Adresse im Feld **Feste IP-Adresse** ein.

Zweiter ISPName des Anbieters - Geben Sie den Namen des zweiten ISPs ein.

Einwahlnummer - Geben Sie die vom ISP mitgeteilte ISDN-Einwahlnummer an.

Benutzername - Geben Sie den von Ihrem ISP mitgeteilten Benutzernamen ein.

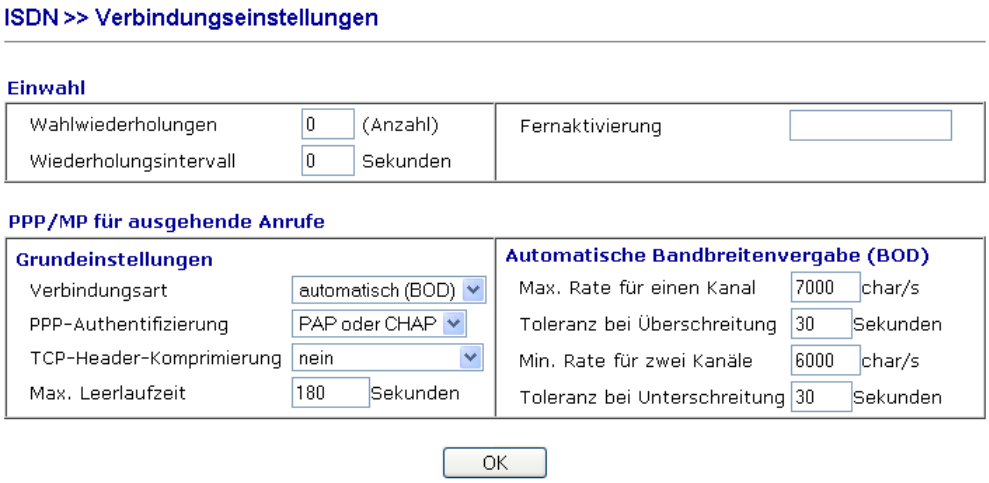
Passwort - Geben Sie das von Ihrem ISP mitgeteilte Passwort ein.

IP-Adresszuweisung (IPCP) durch den zweiten ISP - In den meisten Umgebungen ist es nicht nötig, diese Einstellungen zu ändern, da die meisten ISPs dem Router bei der Einwahl eine dynamische IP-Adresse

zuweisen. Falls Ihnen Ihr ISP eine feste IP-Adresse zuweist, wählen Sie **Ja** und geben die IP-Adresse im Feld **Feste IP-Adresse** ein.

5.11.5 Verbindungseinstellungen

Einige Anwendungen erfordern die Fernaktivierung des Routers bzw. die Fähigkeit, sich über die ISDN-Schnittstelle beim ISP einzuwählen. Vigor-Router unterstützen diese Funktion, indem sie dem Benutzer erlauben, den Router anzurufen und dadurch die Einwahl beim ISP anzustoßen. So ist es einem Teleworker möglich, auf das entfernte Netzwerk zuzugreifen, um vorgehaltene Ressourcen zu nutzen. Natürlich wird für die WAN-Verbindung eine feste IP-Adresse benötigt, und einige interne Netzwerkressourcen wie FTP und WWW müssen für externe Benutzer geöffnet werden.



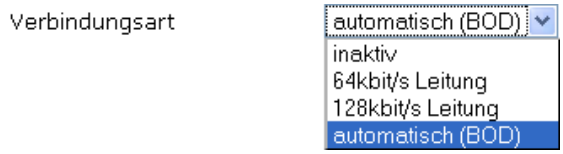
EinwahlWahlwiederholungen - Gibt die Anzahl der Wahlwiederholungen pro anwahlauslösendem Paket an. Ein anwahlauslösendes Paket ist eines, dessen Ziel außerhalb des lokalen Netzwerkes liegt. Die Standardeinstellung ist 0 (keine Wahlwiederholung). Falls dieser Wert auf 5 gesetzt wird, wählt der Router für jedes anwahlauslösende Paket 5 Mal, bis es mit dem ISP oder dem entfernten Zugriffsrouter verbunden ist.

Wiederholungsintervall - Gibt den Zeitraum zwischen Wahlwiederholungen an. Standardmäßig beträgt das 0 Sekunden.

Fernaktivierung – Diese Funktion ist nützlich für Benutzer, die auf den Server in der Zentrale zugreifen möchten, wenn dieser nicht online ist. Um den Server online zu schalten, können die Benutzer den Router über einen Anruf (Nummer ist im Feld Fernaktivierung eingetragen) aktivieren, wodurch die Einwahl ins Internet bzw. die Breitbandverbindung gestartet wird. Der Anruf wird abgebrochen, sobald der Router online ist.

Achten Sie darauf, dass Einwahl über einen ISP richtig konfiguriert ist.

GrundeinstellungenVerbindungsart - Da ISDN über zwei B-Kanäle (64 kbit/s pro Kanal) verfügt, können Sie angeben, ob Sie einen einzigen B-Kanal, zwei B-Kanäle oder BOD (Bandwidth on Demand) wünschen. Es werden vier Optionen angeboten: Inaktiv, 64 kbit/s Leitung, 128 kbit/s Leitung, Automatisch (BOD).



PPP-Authentifizierung - Bestimmt die PPP-Authentifizierungsmethode für PPP/MP-Verbindungen. Aus Kompatibilitätsgründen wählen Sie normalerweise PAP/CHAP.

TCP-Header-Komprimierung - VJ-Komprimierung: **-** Wird für die TCP/IP-Protokoll-Header-Komprimierung verwendet. Setzen Sie diese Option auf Ja, um die Bandbreite bestmöglich auszunutzen.

Max. Leerlaufzeit - Da die IDSN-Verbindungsart auf **Einwahl bei Aufforderung** gesetzt ist, wird die Verbindung nur bei Bedarf aufgebaut.

Automatische Bandbreitenvergabe (BOD) - Die automatische Bandbreitenvergabe wird für Multiple-Link PPP (ML-PPP oder MP) verwendet. Die Parameter werden nur angewendet, wenn Sie die Verbindungsart auf Automatisch (BOD) setzen. Ist dies der Fall, so verwendet ISDN für den Zugriff auf das Internet oder externe Netzwerk normalerweise nur einen B-Kanal. Der Router nimmt die Aktivierung/Trennung des zusätzlichen B-Kanals anhand der hier konfigurierten Parameter vor. Beachten Sie, dass der char/s-Wert (characters per second) die gesamte Linknutzung beinhaltet.

Max. Rate für einen Kanal und Toleranz bei Überschreitung - Diese Parameter geben an, wann der zweite Kanal zu aktivieren ist. Wenn die Auslastung des ersten verbundenen Kanals die Schwelle für den angegebenen Zeitraum überschreitet, wird der zweite Kanal aktiviert. Die Gesamtgeschwindigkeit beträgt somit 128 kbit/s (zwei B-Kanäle).

Min. Rate für zwei Kanäle und Toleranz bei Unterschreitung - Diese Parameter geben an, wann der zweite Kanal zu trennen ist. Wenn die Auslastung der zwei B-Kanäle die

Schwelle für den angegebenen Zeitraum unterschreitet, wird der zweite Kanal getrennt. Die Gesamtgeschwindigkeit beträgt somit 64 kbit/s (ein B-Kanal).

5.12 TK-Anlage

Die TK-Anlage ist ein privates Telefonnetzwerk, das in einem Unternehmen eingesetzt werden kann. Teilnehmer der TK-Anlage können eine gewisse Anzahl an ausgehenden Leitungen für externe Anrufe gemeinsam nutzen.

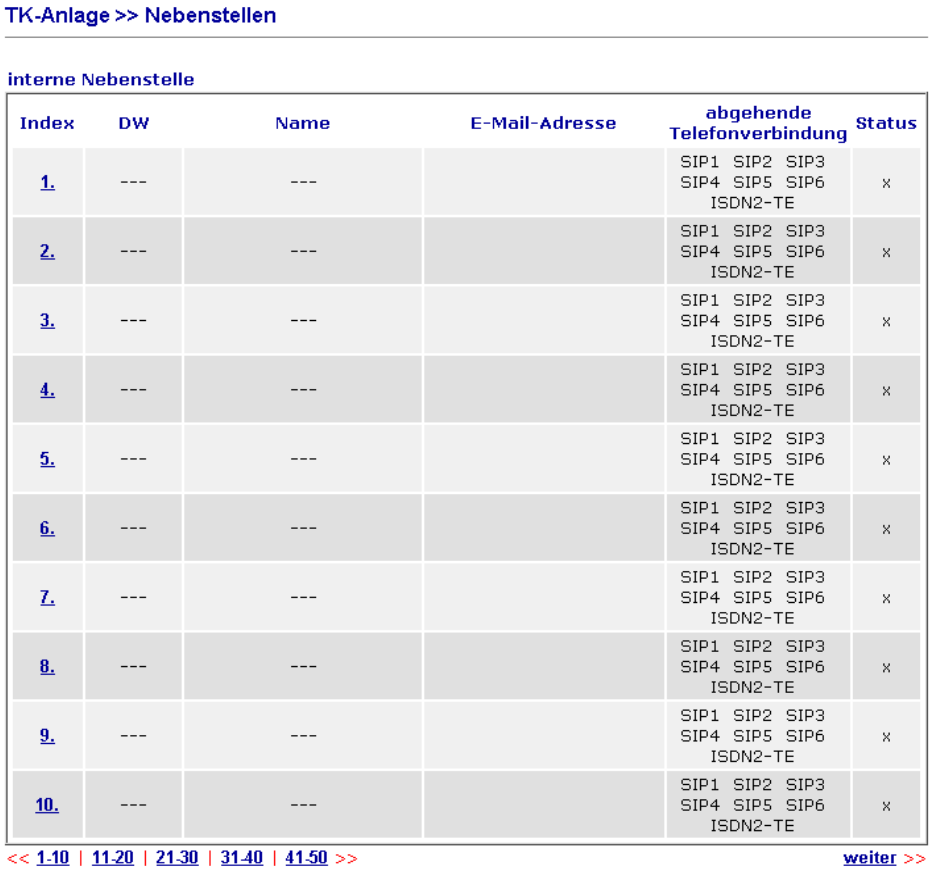
Die TK-Anlage verbindet die Vorteile von VoIP, indem Sie die Anrufe vom IP-Telefon über das IP-Netzwerk in Daten überleitet, die von konventionellen TK-Anlagen verarbeitet werden können. Mit Hilfe dieser neuartigen Plattform können Unternehmen das Datennetzwerk zur Sprachübertragung nutzen. Um den Standort des IP-Telefonapparates zu ändern, braucht ein Teilnehmer den Apparat lediglich mit einem anderen Netzwerkanschluss verbinden. Auf diese Weise werden Vorgänge wie Umzug, Neuanlage, Änderung und Löschung von Telefoneinstellungen vereinfacht. Außerdem ist die Verbindung mit anderen Systemen wie Call Centern möglich, um eine multifunktionelle Kommunikationsplattform bereitzustellen. Diese TK-Anlage trägt auch zu großen Kosteneinsparungen in der Unternehmenskommunikation bei.

Mit Hilfe dieses Menüs können Sie die meisten Einstellungen der TK-Anlage konfigurieren.

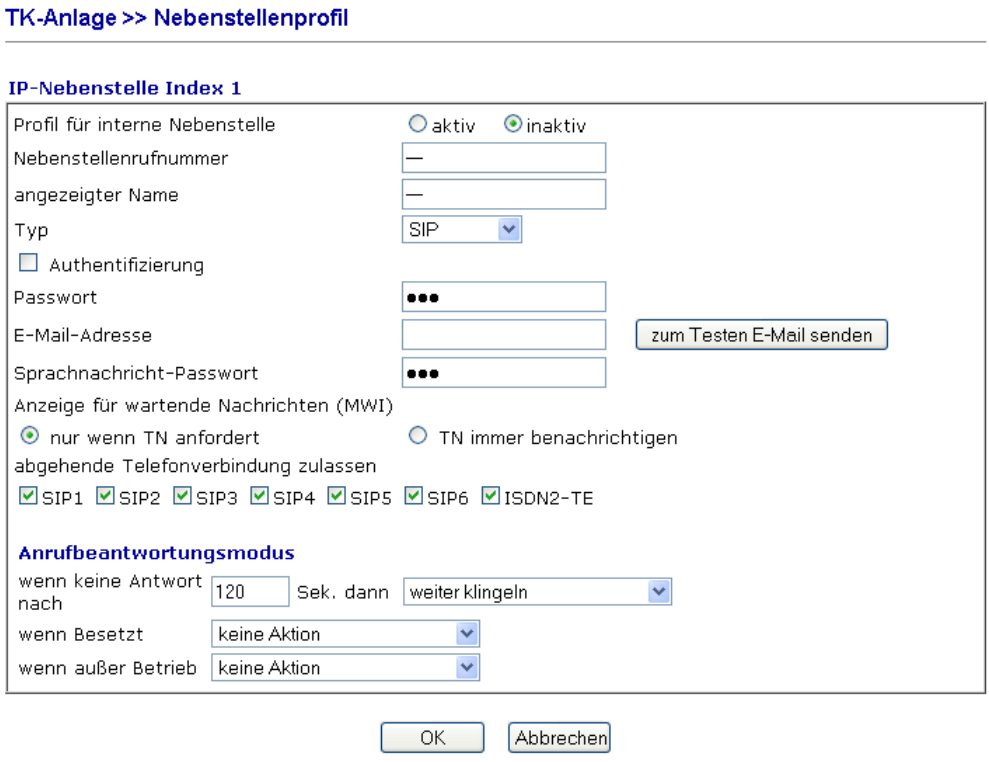
Die folgende Abbildung zeigt die Menüeinträge für die TK-Anlage:

5.12.1 Nebenstellen

Das System erlaubt die Einrichtung von bis zu 50 Nebenstellenrufnummern. Öffnen Sie **TK-Anlage>>Nebenstellen**, um auf die folgenden Seiten zu gelangen.


TK-Anlage >> Nebenstellen
interne Nebenstelle
Index
DW
Name
E-Mail-Adresse
abgehende Telefonverbindung
Status
1. --- --- SIP1 SIP2 SIP3 SIP4 SIP5 SIP6 ISDN2-TE x
2. --- --- SIP1 SIP2 SIP3 SIP4 SIP5 SIP6 ISDN2-TE x
3. --- --- SIP1 SIP2 SIP3 SIP4 SIP5 SIP6 ISDN2-TE x
4. --- --- SIP1 SIP2 SIP3 SIP4 SIP5 SIP6 ISDN2-TE x
5. --- --- SIP1 SIP2 SIP3 SIP4 SIP5 SIP6 ISDN2-TE x
6. --- --- SIP1 SIP2 SIP3 SIP4 SIP5 SIP6 ISDN2-TE x
7. --- --- SIP1 SIP2 SIP3 SIP4 SIP5 SIP6 ISDN2-TE x
8. --- --- SIP1 SIP2 SIP3 SIP4 SIP5 SIP6 ISDN2-TE x
9. --- --- SIP1 SIP2 SIP3 SIP4 SIP5 SIP6 ISDN2-TE x
10. --- --- SIP1 SIP2 SIP3 SIP4 SIP5 SIP6 ISDN2-TE x
<< 1-10 | 11-20 | 21-30 | 31-40 | 41-50 >>
weiter >>

Es sind 10 Gruppen von Nebenstellenrufnummern konfigurierbar. Klicken Sie eine Nummer unter Index an, um zur Detailkonfiguration zu gelangen.



Profil für interne Nebenstelle - Klicken Sie auf **Aktiv**, um dieses Profil zu aktivieren.

Nebenstellenrufnummer - Geben Sie die Nebenstellenrufnummer für den Index an.

Benutzername - Geben Sie den anzuzeigenden Namen für dieses Nebenstellenprofil ein.

Authentifizierung - Markieren Sie dieses Kästchen, damit die TK-Anlage beim Wählen der Nummer die Authentifizierung durchführt.

Passwort - Geben Sie für die TK-Anlage eine Nummer für die Authentifizierung an. Wenn sich ein IP-Telefon mit dem Netzwerk verbindet, verwendet die TK-Anlage dieses Passwort für die Authentifizierung.

E-Mail-Adresse - Geben Sie die E-Mail-Adresse an, an die bei eingehenden Anrufen die Sprachnachrichten gesendet werden sollen.

Test-E-Mail versenden: - Klicken Sie auf diese Schaltfläche, um eine Test-Nachricht an die eingegebene E-Mail-Adresse zu senden.

Sprachnachricht-Passwort - Geben Sie hier ein Passwort ein. Der Benutzer wird aufgefordert, dieses Passwort einzugeben, um seine Sprachnachrichten anhören zu können.

Anzeige für wartende Nachrichten (MWI) - Die Teilnehmer haben die Wahl zwischen zwei MWI-Typen. Wählen Sie den Ihren Anforderungen entsprechenden Typ.

Nur wenn TN anfordert - Der Teilnehmer muss zunächst eine Anforderung stellen (SUBSCRIBE). Wenn die TK-Anlage eine neue Sprachmitteilung von einer Nebenstelle entdeckt oder der Zustand der Sprachmitteilung geändert wird, sendet sie innerhalb der gültigen Anforderungszeit eine Nachricht an die entsprechenden Teilnehmer (NOTIFY).

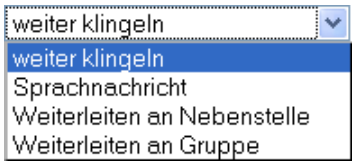
TN immer benachrichtigen - Der Teilnehmer wird benachrichtigt, auch wenn er dies nicht explizit anfordert. Die TK-Anlage benachrichtigt die Teilnehmer, sobald eine neue Nachricht vorliegt oder der Teilnehmer sich erneut an der TK-Anlage anmeldet.

Abgehende Telefonverbindung zulassen - Es stehen für diese Verbindung sechs externe Leitungen (SIP-Konten) und zwei ISDN-

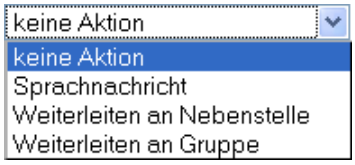
Leitungen (je nach Konfiguration der Telefoneinstellungen) zur Verfügung. Bitte markieren Sie die gewünschten Leitungen.

Anrufbeantwortungsmodus - Geben Sie an, wie mit eingehenden Anrufen umgegangen werden soll.

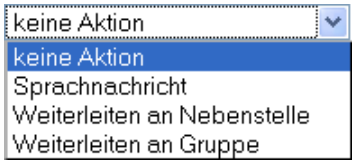
Wenn keine Antwort nach ….. – Falls ein eingehender Anruf nicht abgenommen wird, kann er gehalten oder zu einer anderen Nebenstelle oder Gruppe umgeleitet werden. Bitte geben Sie die Wartezeit sowie die durchzuführende Aktion an.



Wenn besetzt – Falls diese Nebenstelle besetzt ist, können Sie eingehende Anrufe zu einer anderen Nebenstelle oder Gruppe umleiten.



Wenn außer Betrieb – Wenn diese Nebenstelle außer Betrieb ist, können Sie eingehende Anrufe zu einer anderen Nebenstelle oder Gruppe weiterleiten.



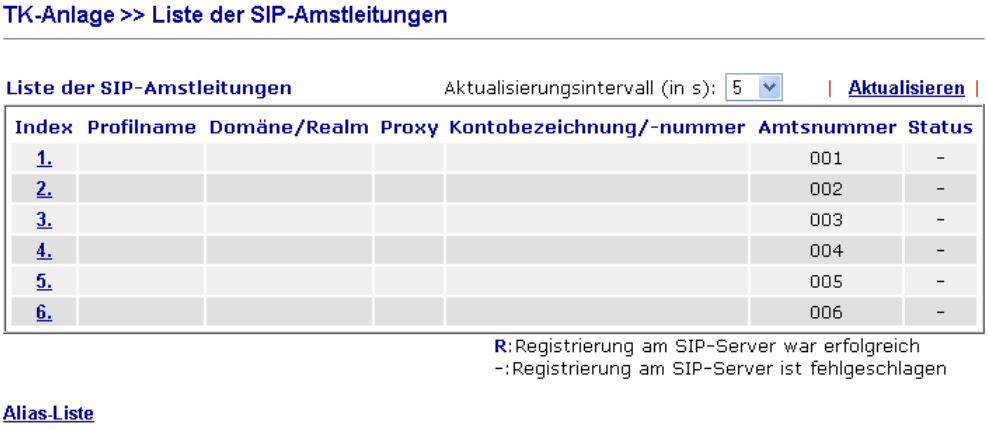
5.12.2 Leitungseinstellungen

Diese TK-Anlage bietet sechs externe SIP-Leitungen und zwei ISDN-Leitungen. Die Teilnehmer können diese unter SIP-Amtsleitung und ISDN-Amtsleitung einstellen.

DID (Direct Inward Dialing) ist ein Dienst, der von SIP-Anbietern zur Verfügung gestellt wird. Dieser Dienst ermöglicht ein SIP-Hauptkonto (**SIP-Amtsleitung**) mit mehreren Unterkonten (eingerichtet in der **Alias-Liste** unter **SIP-Amtsleitung**). Wenn die Hauptkonten auf dem VigorIPPBX 2820 registriert sind, verfügt der Router gleichzeitig auch über diese Unterkonten. So können sowohl die SIP-Hauptkonten als auch die Unterkonten über den VigorIPPBX 2820 angewählt werden.

5.12.2.1 SIP-Amtsleitung

Auf dieser Seite können Sie bis zu sechs SIP-Amtsleitungen (Hauptkonto) und 50 Alias-Namen (Unterkonten) einrichten.



Profilname - Zeigt den Namen des Hauptkontos an.

Domain/Bereich - Zeigt den Domain-Namen oder die IP-Adresse des SIP-Registrar-Servers an.

Proxy - Zeigt den Domain-Namen oder die IP-Adresse des SIP-Proxy-Servers an.

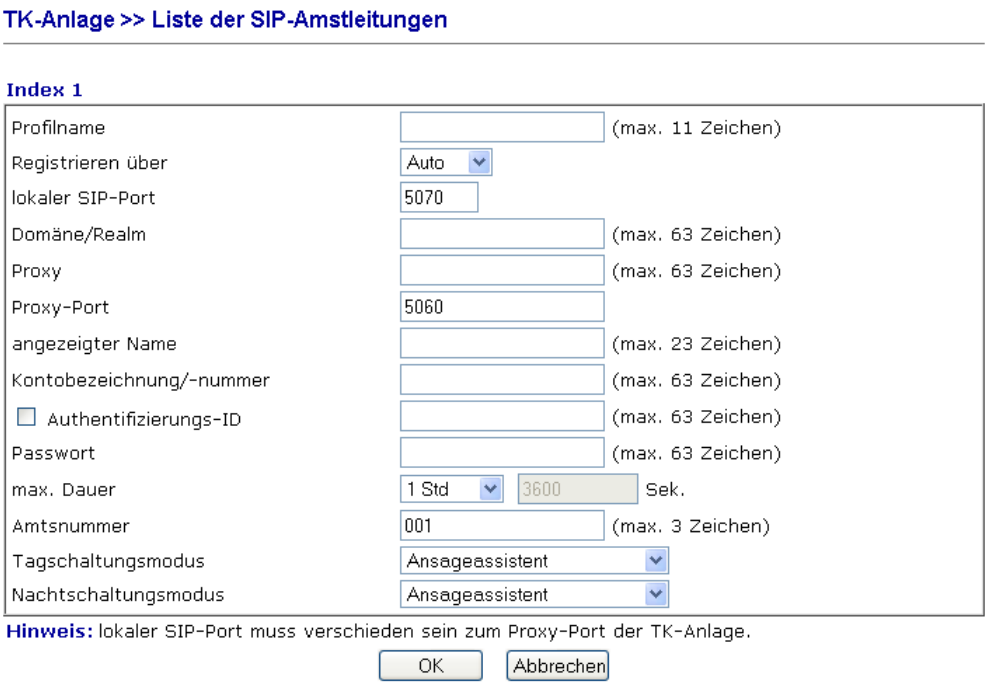
Kontobezeichnung/-nummer - Zeigt die Kontobezeichnung der SIP-Adresse an.

Amtsnummer - Zeigt die Amtsnummer für das Konto an.

Status - Zeigt den aktuellen Status des Kontos an (Anmeldung erfolgreich oder fehlgeschlagen).

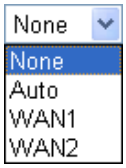
Alias-Liste - Hier können Sie Unterkonten für die Hauptkonten der SIP-Amtsleitung einrichten.

Klicken Sie eine Nummer unter Index an, um zur Detailkonfiguration zu gelangen.



Profilname - Geben Sie für dieses Profil eine Bezeichnung zur Identifizierung ein. Der Name kann ähnlich wie der Profilname lauten. Wenn der Domain-Name beispielsweise *draytel.org* ist, können Sie in diesem Feld *draytel-1* eingeben.

Registrieren über - Falls Sie VoIP-Anrufe tätigen möchten, ohne persönliche Angaben zu machen, wählen Sie **Keine** und markieren das entsprechende Kästchen. Manche SIP-Server erlauben den Teilnehmern, die VoIP-Funktion ohne Registrierung zu nutzen. Wir empfehlen die Einstellung **Auto**. In diesem Fall wählt das System einen geeigneten Weg für Ihre VoIP-Anrufe.



SIP-Port - Bestimmen Sie die Port-Nummer, auf der die SIP-Nachrichten zum Aufbau einer Sitzung gesendet/empfangen werden sollen. Der Standardwert ist **6060.** Die Gegenstelle muss bei ihrem Registrar den gleichen Wert einstellen.

Domain/Bereich - Setzen Sie hier den Domain-Namen oder die IP-Adresse des SIP-Registrar-Servers.

Proxy - Setzen Sie den Domain-Namen oder die IP-Adresse des SIP-Proxy-Servers. Sie können nach dem Domain-Namen die Port-Nummer in der Form **:Port-Nummer** angeben,

um den entsprechenden Port als Ziel der Datenübertragung zu bestimmen (z.B. **nat.draytel.org:5065**).

Proxy-Port - Hier können Sie die Port-Nummer für den Proxy-Server bestimmen.

Angezeigter Name - Die Anrufer-ID, die auf dem Display Ihres Gesprächspartners angezeigt werden soll.

Kontobezeichnung/-nummer - Geben Sie die SIP-Kontobezeichnung ein, d.h. den Text vor @..

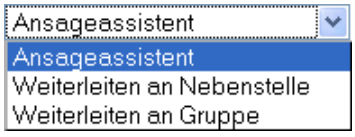
Authentifizierungs-ID - Markieren Sie das Kästchen, um diese Funktion zu aktivieren, und geben Sie den Namen oder die Nummer ein, der/die für die SIP-Authentifizierung am SIP-Registrar verwendet wird. Falls diese Einstellung der Kontobezeichnung entspricht, können Sie darauf verzichten, dieses Kästchen zu markieren und einen Wert in das Feld zu schreiben.

Passwort - Das Passwort, das Ihnen im Zuge der Anmeldung bei einem SIP-Dienst mitgeteilt wurde.

Max. Dauer - Dies gibt die Dauer an, für welche Ihr SIP-Registrar-Server Ihren Registrierungseintrag aufrecht erhält. Vor Ablauf dieser Zeit sendet der Router erneut eine Registrierungsanforderung an den SIP-Registrar.

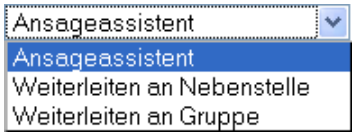
Amtsnummer - Eine Nebenstelle kann auf zweierlei Weise auf die Amtsleitung zugreifen. Der erste Ansatz besteht darin, die Nummer für die Amtsleitung zu wählen und etwas zu warten. Sobald das Amtszeichen ertönt, kann die tatsächliche externe Telefonnummer gewählt werden. Alternativ können die Nummer für die Amtsleitung und dann die tatsächliche externe Rufnummer gewählt werden, ohne auf das Amtszeichen zu warten. Die Nummer für die Amtsleitung wird als Amtsnummer bezeichnet.

Tagschaltungsmodus - Hier können Sie den Beantwortungsmodus für die Amtsleitung während der Arbeitszeit einstellen. Sie können den Ansageassistenten (AA) wählen oder Anrufe direkt an eine beliebige Nebenstelle oder Gruppe weiterleiten lassen.



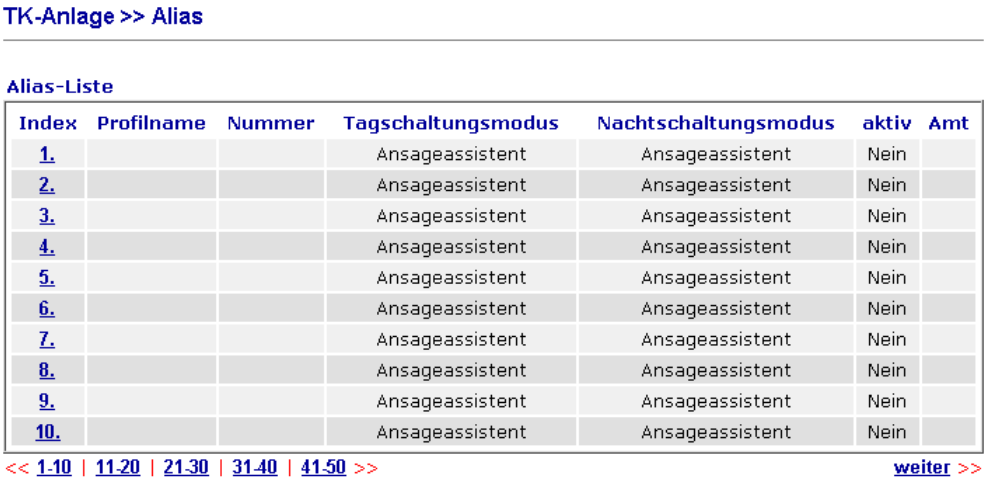
Nachtschaltungsmodus - Hier können Sie den Beantwortungsmodus für die Amtsleitung

außerhalb der Arbeitszeit einstellen. Sie können den Ansageassistenten (AA) wählen oder Anrufe direkt an eine beliebige Nebenstelle oder Gruppe weiterleiten lassen.



Alias-Liste

Klicken Sie auf **Alias-Liste**, um auf die folgende Konfigurationsseite zu gelangen:



Profilname - Zeigt den Alias-Namen für das Unterkonto an.

Nummer - Zeigt die Telefonnummer dieses Kontos an.

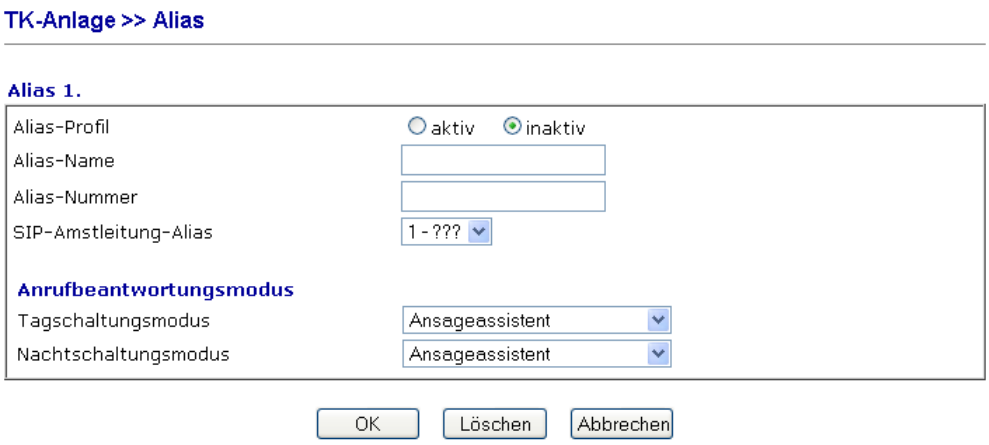
Tagschaltungsmodus - Zeigt den gewählten Anrufbeantwortungsmodus während der Arbeitszeit an.

Nachtschaltungsmodus - Zeigt den gewählten Anrufbeantwortungsmodus außerhalb der Arbeitszeit an.

Aktiv - Zeigt den aktuellen Aktivierungsstatus für das Konto an (aktiv oder inaktiv).

Amt - Zeigt die SIP-Amtsleitung für das Unterkonto an.

Sie können bis zu 50 Profile als Alias für die Liste der SIP-Amtsleitungen setzen. Klicken Sie auf eine Nummer unter Index, um zur Detailkonfiguration zu gelangen.



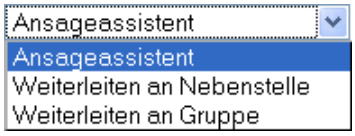
Aktiv - Klicken Sie auf **Aktiv**, um den Eintrag zu aktivieren, oder klicken Sie auf **Inaktiv**, um ihn zu deaktivieren.

Alias - Geben Sie für das Konto einen Namen ein.

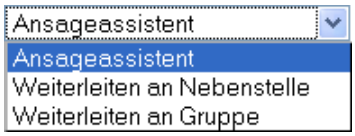
Alias-Nummer - Geben Sie für das Konto eine Nummer ein.

SIP-Amtsleitung-Alias - Wählen Sie für dieses Alias-Profil einen der Punkte von der Liste der SIP-Amtsleitungen.

Tagschaltungsmodus - Hier können Sie den Beantwortungsmodus für die Amtsleitung während der Arbeitszeit einstellen. Sie können den Ansageassistenten (AA) wählen oder Anrufe direkt an eine beliebige Nebenstelle oder Gruppe weiterleiten lassen.

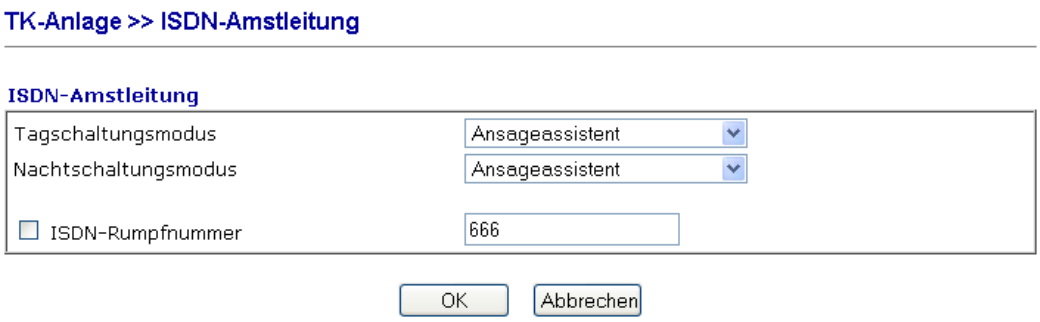


Nachtschaltungsmodus - Hier können Sie den Beantwortungsmodus für die Amtsleitung außerhalb der Arbeitszeit einstellen. Sie können den Ansageassistenten (AA) wählen oder Anrufe direkt an eine beliebige Nebenstelle oder Gruppe weiterleiten lassen.

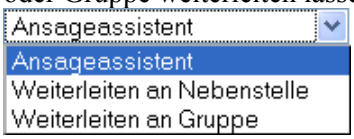


5.12.2.2 ISDN-Amtsleitung

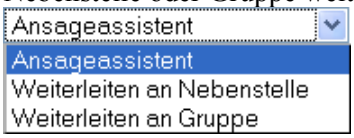
Auf dieser Seite können Sie die ISDN-Amtsleitung einrichten.



Tagschaltungsmodus - Hier können Sie den Beantwortungsmodus für die Amtsleitung während der Arbeitszeit einstellen. Sie können den Ansageassistenten (AA) wählen oder Anrufe direkt an eine beliebige Nebenstelle oder Gruppe weiterleiten lassen.



Nachtschaltungsmodus - Hier können Sie den Beantwortungsmodus für die Amtsleitung außerhalb der Arbeitszeit einstellen. Sie können den Ansageassistenten (AA) wählen oder Anrufe direkt an eine beliebige Nebenstelle oder Gruppe weiterleiten lassen.



ISDN-Rumpfnummer - Wenn beide ISDN-Ports auf den TE-Modus gesetzt wurden, können Sie eine Rumpfnummer angeben. Wenn jemand über eine Nebenstelle das ISDN-Netzwerk durch diese Nummer anwählen möchte, sucht der Router automatisch nach einer verfügbaren Leitung.

5.12.3 Telefonbuch

TK-Anlage >> Wählregeln

Konfiguration der Wählregeln

Wählplan
Wahlsperre

5.12.3.1 Wählplan

Auf dieser Seite können Teilnehmer die Vorwahl für das SIP-Konto bearbeiten, indem sie Ziffern hinzufügen, abziehen oder ersetzen. Auf diese Weise können die Teilnehmer einfacher und schneller über die VoIP-Schnittstelle wählen.

TK-Anlage >> Wählplan

Wählplan

#	Aktiv	Vorwahl	Modus	OP-Nummer	min. Länge	max. Länge	Route
1	☐		aus		0	0	ISDN2-TE
2	☐		aus		0	0	ISDN2-TE
3	☐		aus		0	0	ISDN2-TE
4	☐		aus		0	0	ISDN2-TE
5	☐		aus		0	0	ISDN2-TE
6	☐		aus		0	0	ISDN2-TE
7	☐		aus		0	0	ISDN2-TE
8	☐		aus		0	0	ISDN2-TE
9	☐		aus		0	0	ISDN2-TE
10	☐		aus		0	0	ISDN2-TE
11	☐		aus		0	0	ISDN2-TE
12	☐		aus		0	0	ISDN2-TE
13	☐		aus		0	0	ISDN2-TE
14	☐		aus		0	0	ISDN2-TE
15	☐		aus		0	0	ISDN2-TE
16	☐		aus		0	0	ISDN2-TE
17	☐		aus		0	0	ISDN2-TE
18	☐		aus		0	0	ISDN2-TE
19	☐		aus		0	0	ISDN2-TE
20	☐		aus		0	0	ISDN2-TE

Hinweis: The length for Min Len and Max Len fields should be between 0~25.

Tips for One stage dialing for trunk line:
1. Set the mode to "Strip".
2. Let the OP number and Prefix number be the same.
3. Set a suitable range for the length fields.
4. Select a specific route for this rule.

For example, set op number and prefix number to 1, and set the route to VoIP1. When an extension dial "12345", PBX will dial "2345" to the route of VoIP1.

OK Abbrechen

Aktiv - Markieren Sie dieses Kästchen, um diese Einstellung zu aktivieren.

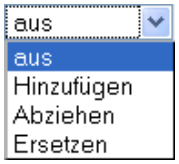
Vorwahl - Die hier eingegebene Telefonnummer wird zur OP-Nummer hinzugefügt, davon abgezogen oder damit ersetzt.

ModusAus - Keine Aktion.

Hinzufügen - Wählen Sie diesen Modus, so wird die eingegebene Nummer beim Wählen über die jeweilige VoIP-Schnittstelle vor die OP-Nummer gestellt..

Abziehen - Wählen Sie diesen Modus, so wird die eingegebene Nummer beim Wählen über die jeweilige VoIP-Schnittstelle von der OP-Nummer abgezogen. Im obigen Beispiel (Prefix-Tabelle) wird die OP-Nummer "886" komplett gelöscht, da die Vorwahl "886" ist.

Ersetzen - Wählen Sie diesen Modus, so ersetzt die eingegebene Nummer beim Wählen über die jeweilige VoIP-Schnittstelle die OP-Nummer. Im obigen Beispiel (Prefix-Tabelle) wird die Vorwahl "03" ersetzt durch "8863". So wird zum Beispiel die Nummer "031111111" in "88631111111" geändert und an den SIP-Server gesendet.

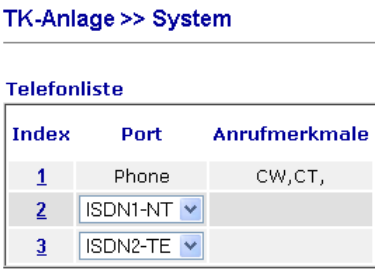


OP-Nummer - Die hier eingegebene Vorwahl stellt den ersten Teil der Kontonummer dar, auf die Sie die Funktion (je nach gewähltem Modus) anwenden möchten.

Min. Länge - Setzen Sie die minimale Länge der zu wählenden Nummer, auf welche die Vorwahleinstellungen angewendet werden sollen. Wenn die zu wählende Nummer im obigen Beispiel (Prefix-Tabelle) 7-9 Stellen hat, können die Vorwahleinstellungen angewendet werden.

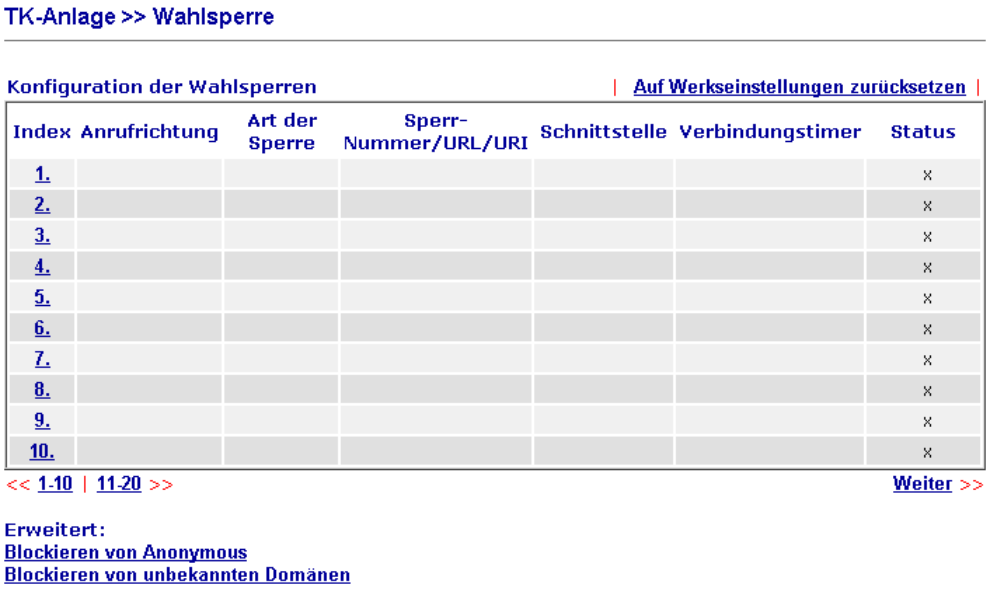
Max. Länge - Setzen Sie die maximale Länge der zu wählenden Nummer, auf welche die Vorwahleinstellungen angewendet werden sollen.

Schnittstelle - Wählen Sie die Schnittstelle, auf der Sie die Vorwahleinstellungen der gespeicherten SIP-Konten anwenden möchten. Richten Sie zunächst ein SIP-Konto ein, um diese Schnittstelle verfügbar zu machen. Dieser Punkt richtet sich nach den Port-Einstellungen unter **TK-Anlage>>System>>Telefoneinstellungen** und **TK-Anlage>>Leitungseinstellungen>>SIP-Amtsleitung**.

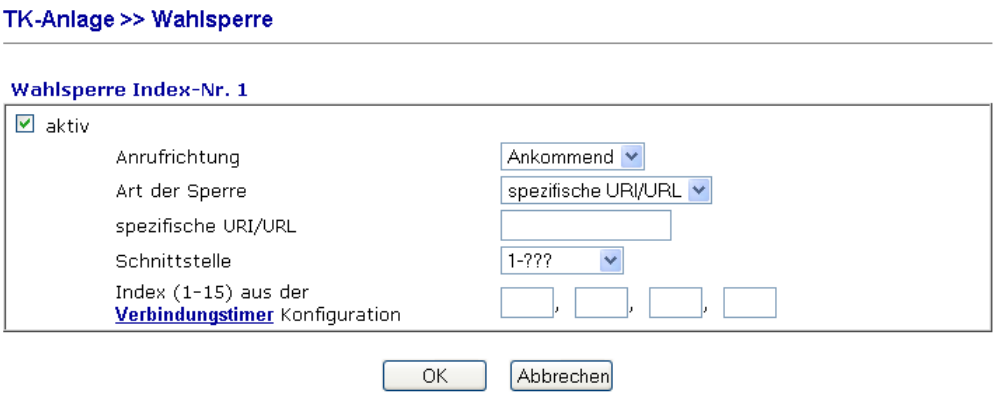


5.12.3.2 Wahlsperre

Die Wahlsperre dient der Sperre von unerwünschten Anrufen.

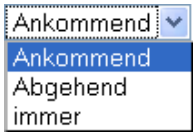


Klicken Sie auf eine Indexnummer, um auf die Telefonbuchseite zu gelangen.

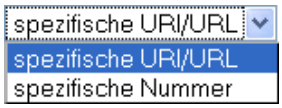


Aktiv - Markieren Sie dieses Kästchen, um diesen Eintrag zu aktivieren.

Anrufrichtung - Hier können Sie die Richtung der Anrufe festlegen: Rein – eingehende Anrufe, Raus – ausgehende Anrufe, Rein & Raus – ein- und ausgehende Anrufe.



Art der Sperre - Hier können Sie die Art der VoIP-Anrufe, URI/URL oder Nummer bestimmen. Je nach Auswahl stehen unterschiedliche Einstellungen zur Verfügung.



Spezifische Nummer/spezifische URI/URL - Dieses Feld ändert sich je nach der Art der gewählten Sperre. Bitte geben Sie eine Nummer oder eine URI/URL ein.

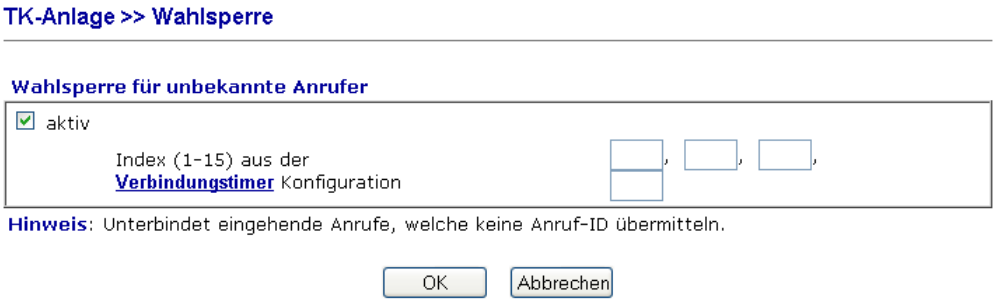
Schnittstelle - "Alle" bedeutet, dass dieser Mechanismus alle Anrufe (ISDN1/2 sowie SIP) blockieren wird. Alternativ können Sie einen bestimmten zu blockierenden Port aus der Dropdown-List wählen.

Index (1-15) aus dem Verbindungstimer - Unter den Indexnummern der Timerprofile können Sie die Wahlsperre einrichten. Das Kapitel **Anwendungen >>Verbindungstimer** enthält Einzelheiten zur Konfiguration.

Außerdem können Sie erweiterte Einstellungen für eine **Blockieren von Anonymous**, **Blockieren von unbekannten Domänen** oder **Blockieren von IP-Adressen** einrichten. Klicken Sie einfach auf die Links, um in die entsprechenden Dialoge zu gelangen.

Blockieren von Anonymous – Diese Funktion kann verwendet werden, um eingehende Anrufe ohne Anrufer-ID auf der im folgenden Fenster angegebenen Schnittstelle zu blockieren. Diese Beschränkung kann auch auf der Grundlage von vorkonfigurierten Listen stattfinden.

Blockieren von unbekannten Domänen – Diese Funktion kann eingehende Anrufe von unbekannten Domänen sperren, die nicht in den SIP-Konten angegeben sind. Diese Beschränkung kann auch auf der Grundlage von vorkonfigurierten Listen stattfinden.

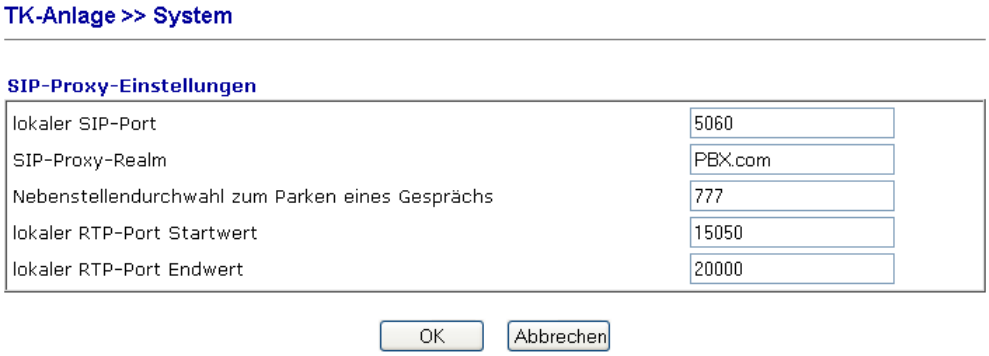


5.12.4 System

Auf dieser Seite können Sie die erweiterten Systemeinstellungen konfigurieren.

5.12.4.1 SIP-Proxy-Einstellungen

Um das IP-Telefon erfolgreich an der TK-Anlage anzumelden, müssen die Teilnehmer die Einstellungen auf dieser Seite konfigurieren.



Lokaler SIP-Port - Setzen Sie eine Port-Nummer als lokalen SIP-Port. Die Standardeinstellung ist 5060.

SIP-Proxy-Realm - Geben Sie den Domain-Namen des SIP-Dienstes ein. Bei einer SIP-URI ist dies der Teil nach dem @ Zeichen.

Nebenstellendurchwahl zum Parken eines Gesprächs - Diese Nummer wird verwendet, um ein Gespräch zu parken. Die standardmäßig eingestellte Nummer ist "777".

1. Wenn Sie einen Anruf empfangen und zum anderen Ende gehen müssen, um mit dem gleichen Anrufer zu sprechen, können Sie den Anruf von Ihrem VoIP-Telefonapparat aus parken und an diese Nummer umleiten.

2. Der Parkserver gibt Ihnen eine andere Sprachnummer (Ihre Parknummer ist z.B. XXXX).

   Bitte merken Sie sich diese Nummer und legen Sie das Telefon auf.

3. Verwenden Sie am anderen Ende

einen anderen Telefonapparat, um mit dem Anrufer weiterzusprechen, in dem Sie die Sprachnummer (XXXX) wählen.

Lokaler RTP-Start-Port/lokaler RTP-Stopp-Port - Falls Ihr VoIP-Anbieter Ihnen diese Informationen gegeben hat, geben Sie bitte die Port-Nummern für den RTP-Verkehr ein. Ansonsten verwenden Sie die Standardeinstellungen. Falls lediglich ein Port verwendet wird, geben Sie in den beiden Feldern die gleiche Nummer ein. Um einen Bereich zu bestimmen geben Sie die erste Nummer im Feld Lokaler RTP-Start-Port und die letzte Nummer im Feld lokaler RTP-Stopp-Port ein.

5.12.4.2 Nebenstellengruppe

Auf dieser Seite können Sie mehrere Nebenstellenrufnummern gruppieren. Bei eingehenden Anrufen klingeln alle Nebenstellenrufnummern einer solchen Gruppe.

TK-Anlage >> System

Nebenstellengruppe

Index	Gruppenname	Gruppendurchwahl	Mitglieder der Gruppe (max. 20 Einträge)
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			

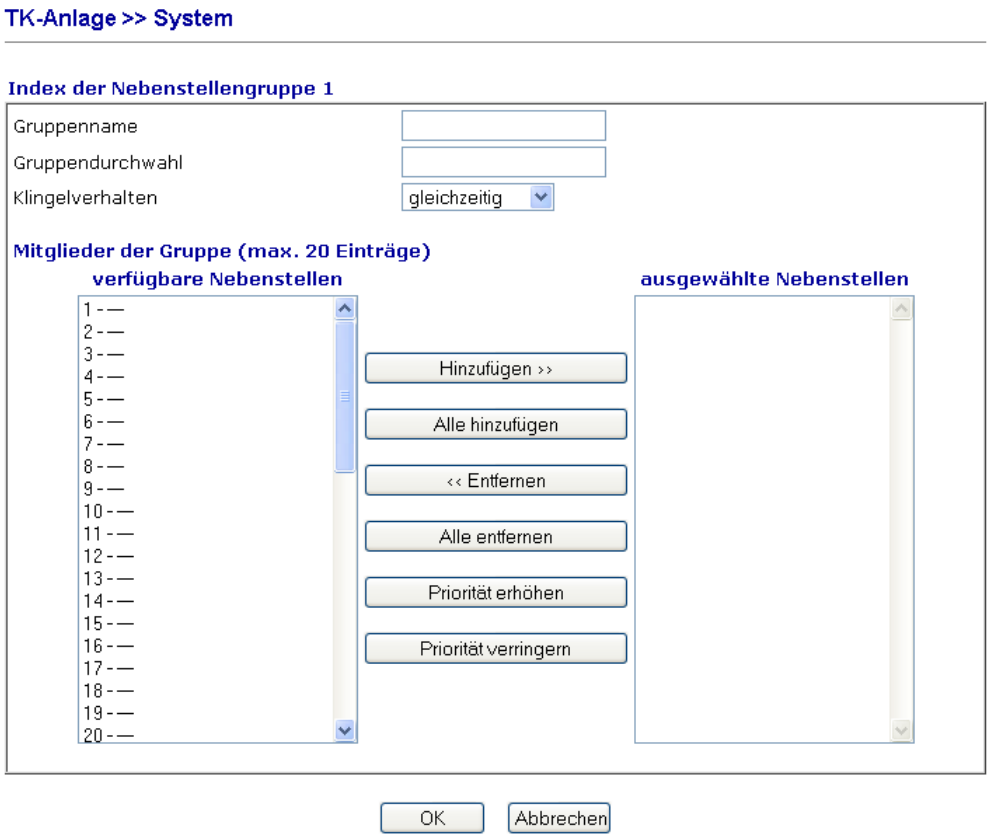
Index - Sie können 10 Gruppen für verschiedene Situationen einrichten. Klicken Sie die Nummern unter Index an, um die Einzelheiten zu konfigurieren.

Gruppenname - Zeigt den Namen der Gruppe an.

Gruppendurchwahl - Zeigt die Durchwahl der Gruppe an.

Mitglieder der Gruppe - Zeigt die Mitglieder in der Gruppe an.

Klicken Sie auf eine Indexnummer, um auf die Seite zur Konfiguration der Nebenstellengruppe zu gelangen.



Gruppenname - Geben Sie einen geeigneten Namen für die Gruppe ein.

Gruppendurchwahl - Geben Sie die Durchwahl für die Gruppe an.

Klingelverhalten - Verwenden Sie das Dropdown-Menü, um das Klingelverhalten zu bestimmen.

Gleichzeitig – Wenn Sie diese Regel wählen, klingeln bei eingehenden Anrufen alle Telefone der Gruppe.

Nacheinander - Wenn Sie diese Regel wählen, klingeln bei eingehenden Anrufen alle Telefone nacheinander.

Hinzufügen - Klicken Sie auf diese Taste, um das gewählte Objekt von der Liste der verfügbaren Nebenstellen zur Liste der ausgewählten Nebenstellen zu verschieben.

Alle hinzufügen - Klicken Sie auf diese Taste, um alle Objekte von der Liste der verfügbaren Nebenstellen zur Liste der ausgewählten Nebenstellen zu verschieben.

Entfernen - Klicken Sie auf diese Taste, um das gewählte Objekt von der Liste der ausgewählten Nebenstellen zur Liste der verfügbaren Nebenstellen zu verschieben.

Alle entfernen - Klicken Sie auf diese Taste, um die Auswahl in der Liste der

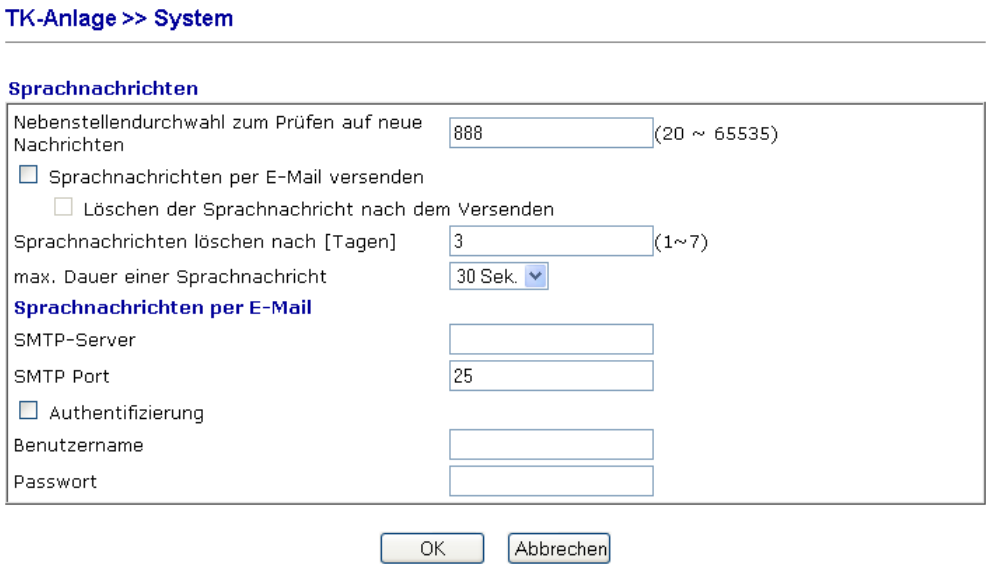
ausgewählten Nebenstellen zu löschen.

Aufwerten - Klicken Sie auf diese Taste, um das gewählte Objekt nach oben zu verschieben.

Abwerten - Klicken Sie auf diese Taste, um das gewählte Objekt nach unten zu verschieben.

5.12.4.3 Sprachnachrichten

Auf dieser Seite können die Teilnehmer den Umgang mit Sprachnachrichten konfigurieren.



Nebenstellendurchwahl zum Prüfen auf neue Nachrichten - Der Teilnehmer kann die hier angegebene Nummer verwenden, um persönliche Sprachnachrichten von der TK-Anlage abzurufen.

Sprachnachrichten per E-Mail versenden - Wenn Sie dieses Kästchen markieren, kann die TK-Anlage die Sprachnachrichten eingehender Anrufe an die angegebene E-Mail-Adresse senden.

Löschen der Sprachnachricht nach dem Versenden - Wenn Sie dieses Kästchen markieren, kann die TK-Anlage die Sprachnachrichten eingehender Anrufe direkt an die angegebene E-Mail-Adresse senden und die temporäre Datei in der TK-Anlage löschen.

Sprachnachrichten löschen nach [Tagen] - Hier geben Sie an, wieviele Tage die Sprachnachrichten aufbewahrt werden sollen.

Max. Dauer einer Sprachnachricht - Geben Sie die Aufnahmelänge für Sprachnachrichten ein.

SMTP-Server - Geben Sie die IP-Adresse oder den Domain-Namen des Servers an, der zum Empfang von Sprachnachrichten verwendet wird.

Authentifizierung - Markieren Sie dieses Kästchen, um den Mail-Server zu authentifizieren.

Benutzername - Geben Sie einen Namen an, mit dem die TK-Anlage den Mail-Server beim Verbindungsaufbau automatisch authentifizieren kann.

Passwort - Geben Sie ein Passwort an, mit dem die TK-Anlage den Mail-Server beim Verbindungsaufbau automatisch authentifizieren kann.

5.12.4.4 Tag-/Nacht-Anrufvariante

Hier können Sie 10 Tag-/Nacht-Anrufvarianten mit Startzeit und Endzeit an Arbeitstagen konfigurieren.

Tag-Variante von - Verwenden Sie das Dropdown-Menü, um die Startzeit zu bestimmen.

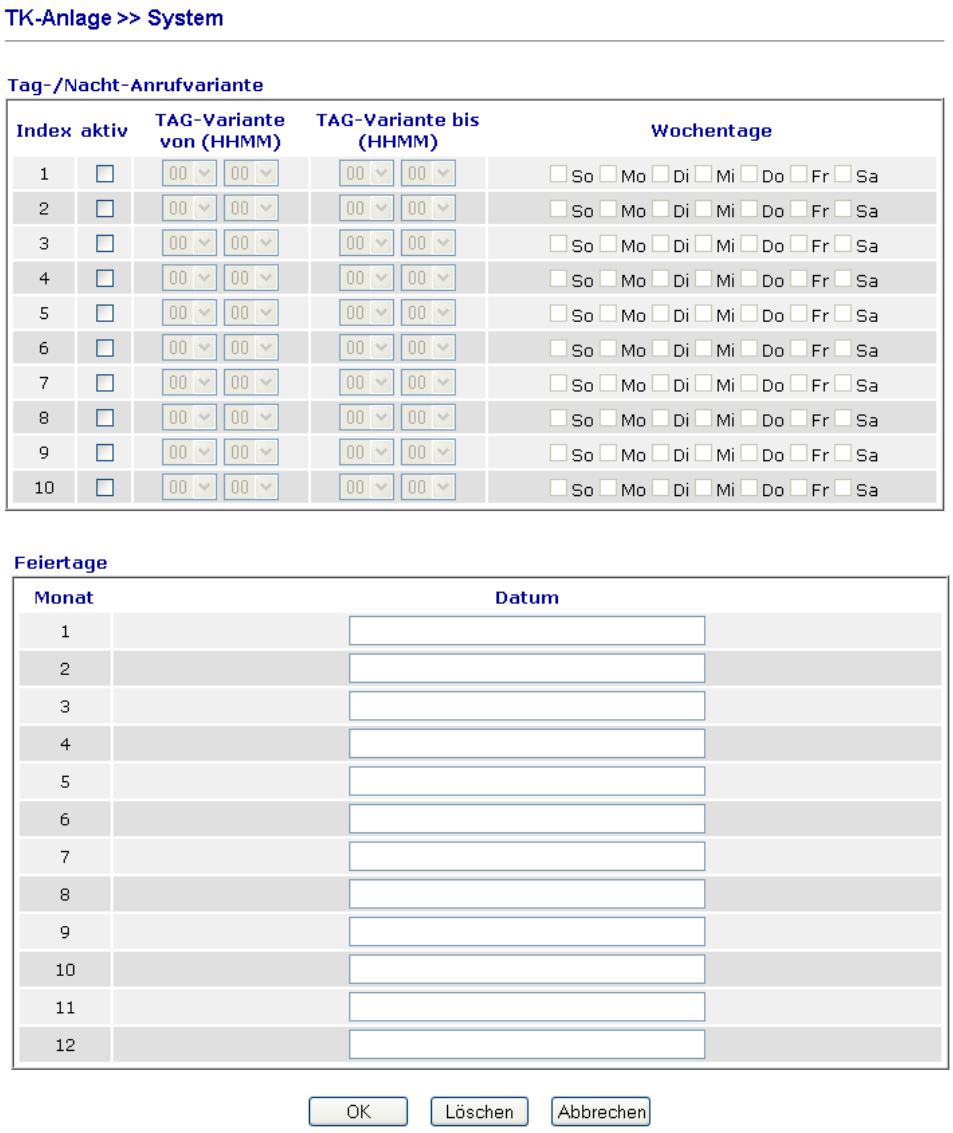
Tag-Variante bis - Verwenden Sie das Dropdown-Menü, um die Schlusszeit zu bestimmen.

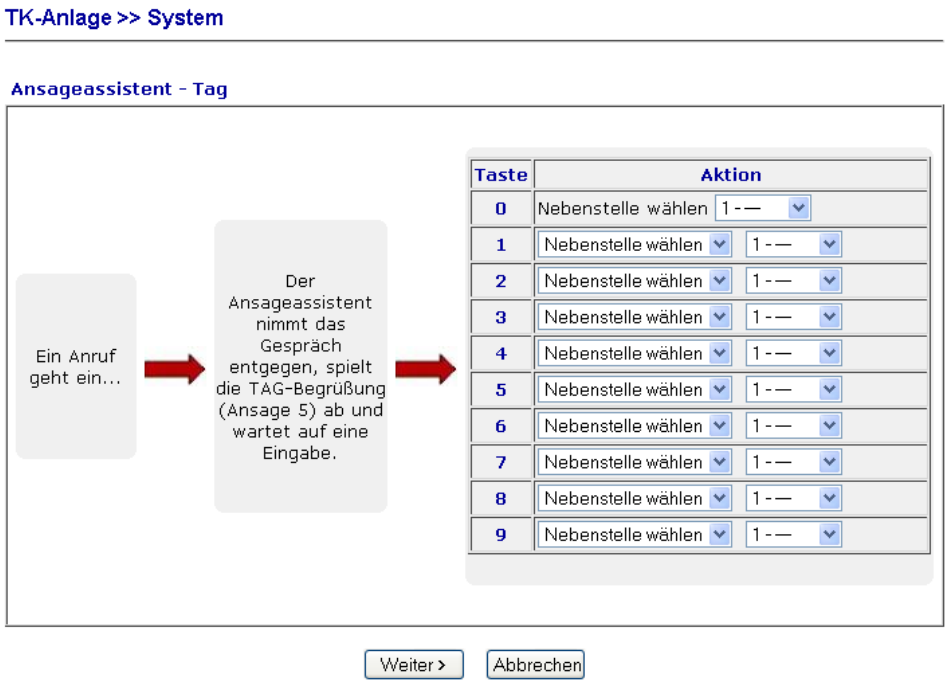
Wochentags - Markieren Sie die Tage, die für die jeweilige Indexnummer als Arbeitszeit gesetzt werden sollen.

Datum - Geben Sie die Daten an, an denen die Einstellungen der Tag-Variante im Urlaub angewendet werden sollen, z.B. 2, 4, 6 und 7 im Datumsfeld für Monat 1. Dies bedeutet, dass die auf dieser Seite konfigurierten Einstellungen der Tagvariante am 2., 4., 6. und 7. Januar angewendet werden.

5.12.4.5 Ansageassistent

Die erste Seite dient der Konfiguration von Anrufen während der Arbeitszeit.




TK-Anlage >> System
Ansageassistent - Tag
Ein Anruf geht ein...
Der Ansageassistent nimmt das Gespräch entgegen, spielt die TAG-Begrüßung (Ansage 5) ab und wartet auf eine Eingabe.
Taste
Aktion
0 Nebenstelle wählen 1 - —
1 Nebenstelle wählen 1 - —
2 Nebenstelle wählen 1 - —
3 Nebenstelle wählen 1 - —
4 Nebenstelle wählen 1 - —
5 Nebenstelle wählen 1 - —
6 Nebenstelle wählen 1 - —
7 Nebenstelle wählen 1 - —
8 Nebenstelle wählen 1 - —
9 Nebenstelle wählen 1 - —
Weiter >
Abbrechen

Klicken Sie auf **Weiter**. Die zweite Seite dient der Konfiguration von Anrufen außerhalb der Arbeitszeit.

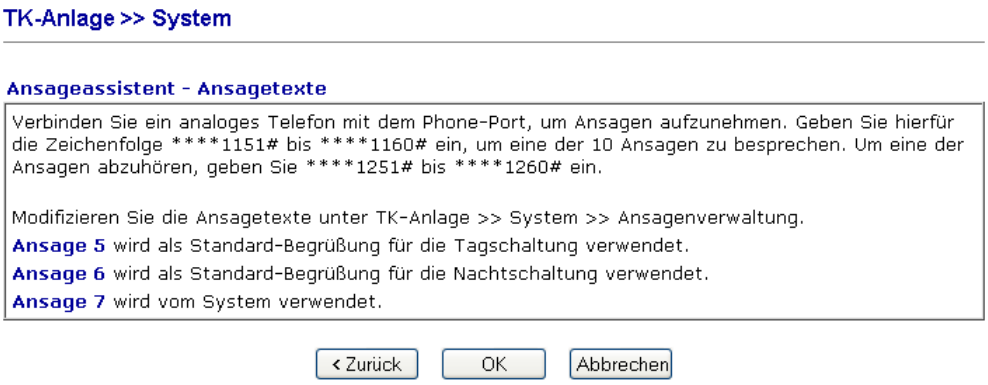
Nebenstelle wählen - Nur die hier gewählte Nebenstellenrufnummer klingelt.

Ansage abspielen - Die Audiodatei wird automatisch abgespielt.

2-9 - Dropdown-Menü 1 enthält die Einträge Nebenstelle wählen/Ansage abspielen/Nebenstellengruppe wählen.

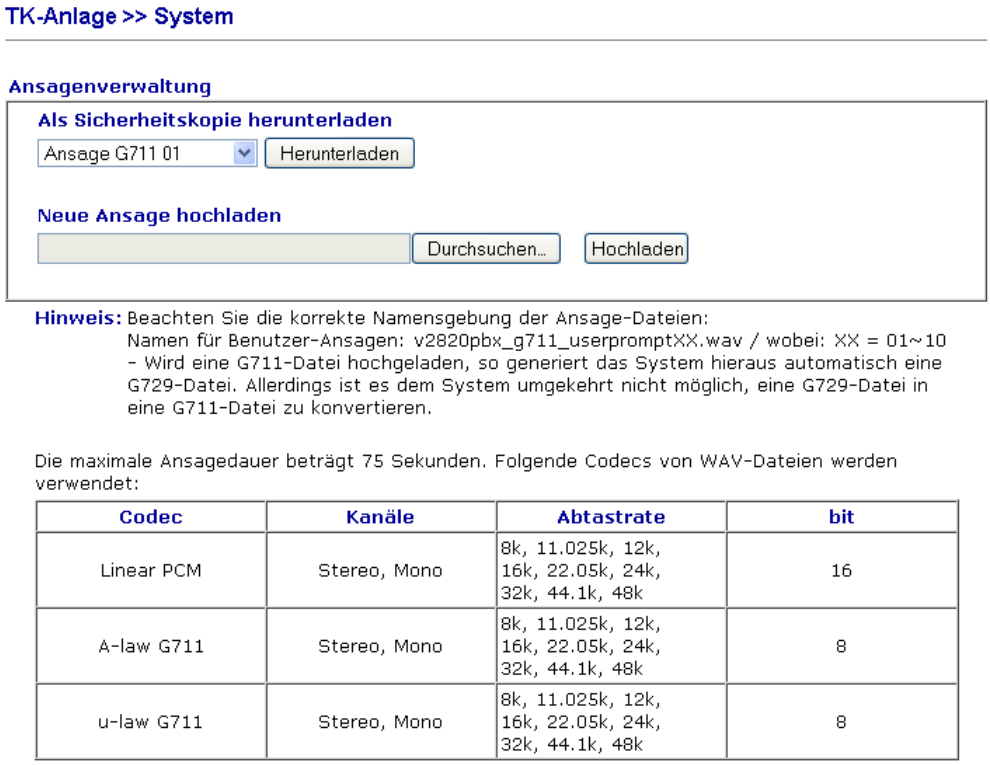
Dropdown-Menü 2 enthält die Bezeichnung der Nebenstelle [(z.B. Tom, Mike)] oder [Ansage 1~ Ansage 10, Audiodateien] oder den Gruppennamen [(z.B. Vertrieb, Entwicklung)]. Die Ansicht ist von der Einstellung in Dropdown-Menü 1 abhängig.

Anschließend erscheint das folgende Fenster:


TK-Anlage >> System
Ansageassistent - Ansagetexte
Verbinden Sie ein analoges Telefon mit dem Phone-Port, um Ansagen aufzunehmen. Geben Sie hierfür die Zeichenfolge ****1151# bis ****1160# ein, um eine der 10 Ansagen zu besprechen. Um eine der Ansagen abzuhören, geben Sie ****1251# bis ****1260# ein.
Modifizieren Sie die Ansagetexte unter TK-Anlage >> System >> Ansagenverwaltung.
Ansage 5 wird als Standard-Begrüßung für die Tagschaltung verwendet.
Ansage 6 wird als Standard-Begrüßung für die Nachtschaltung verwendet.
Ansage 7 wird vom System verwendet.
< Zurück
OK
Abbrechen

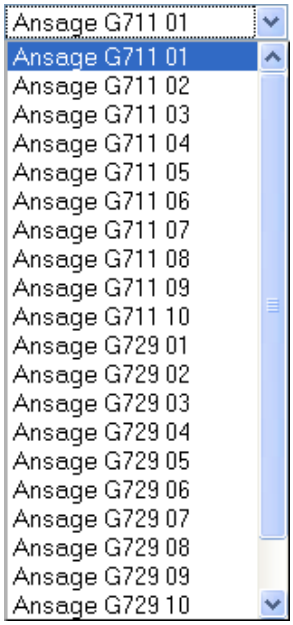
5.12.4.6 Ansagenverwaltung

Die TK-Anlage stellt mehrere Audiodateien bereit, die nach Wahl abgespielt werden können. Weitere Audiodateien können von USD-Speichermedien, Festplatten usw. hochgeladen und auf der TK-Anlage abgespielt werden. Audioaufnahmen können zum Router hochgeladen oder auf den PC heruntergeladen werden. Das Dateiformat der Audiodateien muss jedoch den im Dialog angegebenen Regeln entsprechen. Benutzer können Audiodateien über einen am Router angeschlossenen Telefonapparat oder mit Hilfe eines Aufnahmeprogramms auf dem PC aufnehmen.


TK-Anlage >> System
Ansagenverwaltung
Als Sicherheitskopie herunterladen
Ansage G711 01
Herunterladen
Neue Ansage hochladen
Durchsuchen...
Hochladen
Hinweis: Beachten Sie die korrekte Namensgebung der Ansage-Dateien:
Namen für Benutzer-Ansagen: v2820pbx_g711_userpromptXX.wav / wobei: XX = 01~10
- Wird eine G711-Datei hochgeladen, so generiert das System hieraus automatisch eine G729-Datei. Allerdings ist es dem System umgekehrt nicht möglich, eine G729-Datei in eine G711-Datei zu konvertieren.
Die maximale Ansagedauer beträgt 75 Sekunden. Folgende Codecs von WAV-Dateien werden verwendet:

Codec	Kanäle	Abtastrate	bit
Linear PCM	Stereo, Mono	8k, 11.025k, 12k, 16k, 22.05k, 24k, 32k, 44.1k, 48k	16
A-law G711	Stereo, Mono	8k, 11.025k, 12k, 16k, 22.05k, 24k, 32k, 44.1k, 48k	8
u-law G711	Stereo, Mono	8k, 11.025k, 12k, 16k, 22.05k, 24k, 32k, 44.1k, 48k	8

Download - Die Audiodatei kann im IVR- oder im WAV-Format gespeichert werden. Normalerweise wird die Datei nach der Aufnahme im Speicher des Routers gespeichert. Um die (im Flash-Speicher des Routers gespeicherte(n)) Audiodatei(en) auf Ihren Router zu sichern wählen Sie die entsprechende Datei vom Dropdown-Menü und klicken auf **Herunterladen**.



Die Ansagen 1 bis 10 werden für benutzerdefinierte Audiodateien verwendet (das Dateiformat muss .WAV sein). Die Datei mit den Systemansagen wird von der Router-Firmware bereitgestellt.

Neue Ansage hochladen - Die Datei mit den Systemansagen wird von der Router-Firmware bereitgestellt. Um eine solche Audiodatei zu nutzen, müssen Sie sie nach dem Update der Firmware in den Flash-Speicher des Routers hochladen.

Klicken Sie auf **Durchsuchen**, um andere Audiodateien zu suchen und auszuwählen.

Wiederherstellen - Klicken Sie auf diese Schaltfläche, um die Datei auf dem Router zu speichern. Beim nächsten Mal wird die Audiodatei im TK-System abgespielt.

Hochladen von Ansagen auf Ihren Router

Um die standardmäßige Systemansage zu ändern gehen Sie wie folgt vor:

Führen Sie die bitte die folgenden Schritte durch, um die Systemansagen auf Ihren Router hochzuladen.

1. Bitte verwenden Sie den *DOS-BOX FTP-Client* (in Windows enthaltener FTP-Client), um sich am VigorIPPBX FTP-Server anzumelden.
2. Drücken Sie auf Enter, um sich zu authentifizieren.
3. Geben Sie **put v2820_sysprompt.ivr** ein.
4. Warten Sie etwas. Die Meldung **226 System prompts file has been uploaded successfully** erscheint.
5. Geben Sie **put v2820_g729_sysprompt.ivr** ein.
6. Warten Sie etwas. Die Meldung **226 System prompts G729 file has been uploaded successfully** erscheint.
7. Geben Sie **quit** ein, um den FTP-Client zu schließen. Die Meldung 221 Goodbye! Router will be reboot now erscheint, und der Router startet neu.

Führen Sie bitte die folgenden Schritte durch, um die G729 Benutzeransagen auf Ihren Router hochzuladen:

1. Bitte verwenden Sie den *DOS-BOX FTP-Client* (in Windows enthaltener FTP-Client), um sich am VigorIPPBX FTP-Server anzumelden.
2. Drücken Sie auf Enter, um sich zu authentifizieren.
3. Geben Sie **put v2820_g729_userprompt.ivr** ein.
4. Warten Sie etwas. Die Meldung **226 user prompts G729 file has been uploaded successfully** erscheint.
5. Geben Sie **quit** ein, um den FTP-Client zu schließen. Die Meldung 221 Goodbye! Router will be reboot now erscheint, und der Router startet neu.

Führen Sie bitte die folgenden Schritte durch, um die G729 Benutzeransagen auf Ihren Rechner herunterzuladen:

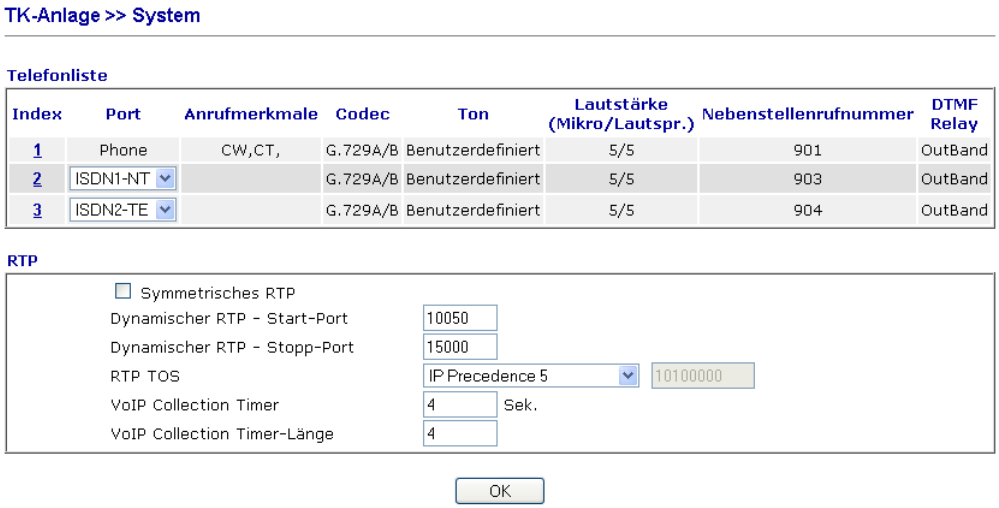
1. Bitte verwenden Sie den *DOS-BOX FTP-Client* (in Windows enthaltener FTP-Client), um sich am VigorIPPBX FTP-Server anzumelden.
2. Drücken Sie auf Enter, um sich zu authentifizieren.
3. Geben Sie **get v2820_G729_userprompt.ivr** ein.
4. Warten Sie etwas. Die Meldung **226 File sent OK** erscheint.
5. Geben Sie **quit** ein, um den FTP-Client zu schließen.

Audiodatei aufnehmen

Das folgende Flussdiagramm zeigt, wie ein Telefonapparat verwendet werden kann, um eine Audiodatei aufzunehmen.

5.12.4.7 Telefoneinstellungen

Auf dieser Seite können die Teilnehmer Telefoneinstellungen konfigurieren.



TelefonlistePort – Sie können hier drei Telefonports konfigurieren. Einer davon (Index 1) ist fest und zwei (Index 2 & 3) sind konfigurierbar. Unter **Telefon**-Port können Sie allgemeine Einstellungen für analoge Telefone konfigurieren. Unter **ISDN**-Port

können Sie allgemeine Einstellungen für die ISDN-Netzwerkverbindung konfigurieren. Die Ports ISDN1 und ISDN2 sind konfigurierbar. Wählen Sie aus der Dropdown-Liste **ISDN1/2-TE** für eine Internet-Verbindung oder **ISDN1/2-S0** (ISDN intern) für ein ISDN-Telefon. Sie können unter gewissen Voraussetzungen sechs Telefone an diesem Router anschließen. Einzelheiten zur ISDN-Telefon-/-Netzwerkverbindung werden in **Abschnitt 1.4** erläutert.

Anrufmerkmale – Eine Kurzbeschreibung der Anrufmerkmale wird zu Ihrer Information in diesem Feld angezeigt.

Codec – Der für jeden Port eingestellte standardmäßige Codec wird zu Ihrer Information in diesem Feld angezeigt. Klicken Sie auf die Nummer unter dem Indexfeld, um die Einstellung für jeden Telefonport zu ändern.

Ton - Toneinstellungen anzeigen, die in den erweiterten Einstellungen der Telefon-Indexnummer konfiguriert wurden.

Lautstärke - Lautstärke für Mikro/Lautsprecher anzeigen, die in den erweiterten Einstellungen der Telefon-Indexnummer konfiguriert wurde.

Standard SIP-Konto – Das Standard SIP-Konto ist "draytel_1". Klicken Sie auf die Nummer unter dem Indexfeld, um das SIP-Konto für jeden Telefonport zu ändern.

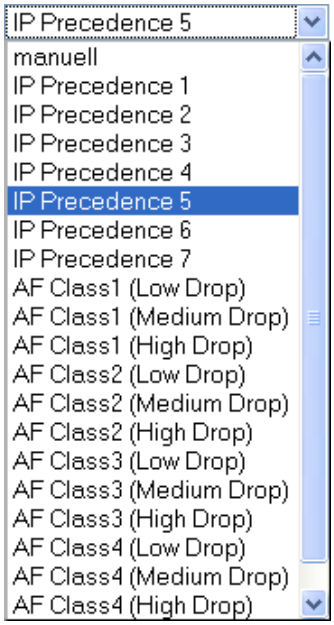
DTMF Relay – DTMF-Modus anzeigen, der in den erweiterten Einstellungen der Telefon-Indexnummer konfiguriert wurde.

RTPSymmetrisches RTP – Markieren Sie dieses Kästchen, um diese Funktion zu aktivieren. Um zu vermeiden, dass die Datenübertragung, die den lokalen Router und den entfernten Router durchläuft, aufgrund der unterschiedlichen IP-Adressen fehlgeleitet wird, können Sie diese Funktion nutzen.

Dynamischer RTP - Start-Port - Gibt den ersten Port für den RTP-Stream an. Der Standardwert ist 10050.

Dynamischer RTP - Stopp-Port - Gibt den letzten Port für den RTP-Stream an. Der Standardwert ist 15000.

RTP TOS – Bestimmt die Stufe der VoIP-Pakete. Verwenden Sie zur Auswahl die Dropdown-Liste.

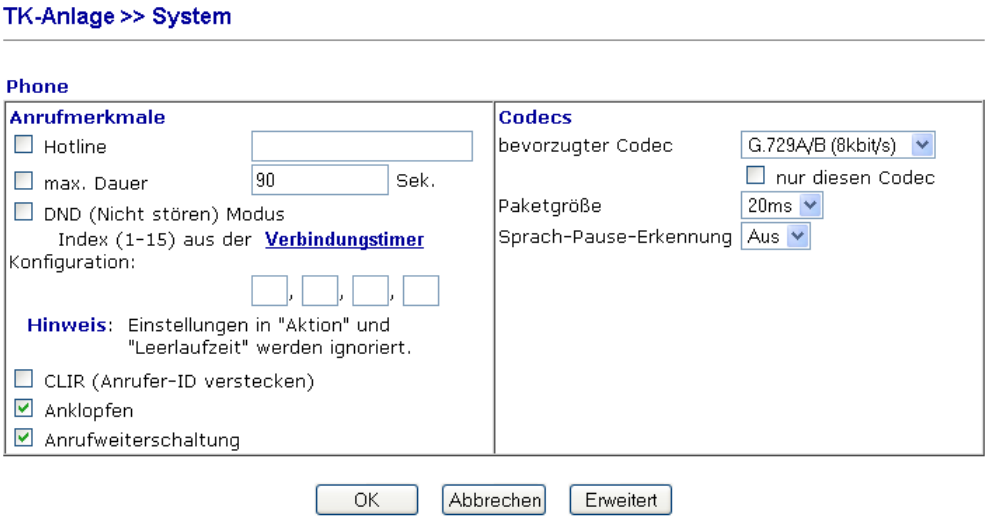


VoIP Collection Timer – Nicht verfügbar.

VoIP Collection Timer-Länge - Nicht verfügbar.

Erweiterte Einstellungen für Telefon-Port

Klicken Sie auf den Link für den Telefon-Port, um auf die Seite zu gelangen, auf der Sie die Telefoneinstellungen konfigurieren können. Die folgende Abbildung zeigt beispielhaft die Seite für einen Telefon-Port.



Hotline - Markieren Sie das Kästchen, um die Funktion zu aktivieren. Geben Sie die SIP-URL im Feld zur automatischen Wahl ein, wenn Sie den Hörer abnehmen.

Max. Dauer - Markieren Sie dieses Kästchen, um diese Funktion zu aktivieren. Falls innerhalb der in diesem Feld angegebenen Zeit keine Antwort erfolgt, wird der Anruf automatisch geschlossen.

DND (nicht stören) Modus - Hier können Sie eine Ruhezeit eingeben, während der Sie nicht durch VoIP-Anrufe gestört werden möchten. Während dieser Zeit hören die Anrufer das Besetztzeichen, der lokale Teilnehmer hört jedoch keinen Klingelton.

Index (1-15) aus dem Verbindungstimer - Unter den Indexnummern gelangen Sie in die Timerprofile, mit denen Sie den DND-Modus steuern können. Kapitel **5.8.2 Verbindungstimer** enthält Einzelheiten zur Konfiguration.

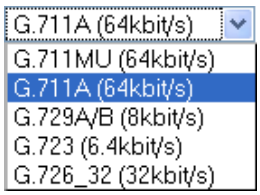
CLIR (Anrufer-ID verstecken) - Markieren Sie dieses Kästchen, um die Anzeige der Anrufer-ID auf dem Display des Telefonapparats zu unterbinden.

Anklopfen - Markieren Sie dieses Kästchen, um diese Funktion zu aktivieren. Ein Hinweiston ertönt, um den Teilnehmer darauf hinzuweisen, dass ein anderer Anruf ansteht. Klicken Sie auf Hook-Flash, um den wartenden Anruf anzunehmen.

Anrufweiterschaltung - Markieren Sie dieses Kästchen, um diese Funktion zu aktivieren. Klicken Sie auf Hook-Flash, um einen anderen Anruf zu tätigen. Falls der Anruf gelingt, legen Sie das Telefon auf. Die anderen beiden Parteien können nun kommunizieren.

Bevorzugter Codec - Hier können Sie einen von fünf Codecs als Standard für Ihre VoIP-Anrufe bestimmen. Der Codec, der für jeden einzelnen Anruf verwendet wird, wird vor jeder Sitzung mit der entfernten Partei ausgehandelt und entspricht eventuell nicht Ihrer Standardwahl. Standardmäßig wird der Codec G.729A/B verwendet, der wenig Bandbreite in Anspruch nimmt aber trotzdem gute Sprachqualität bietet.

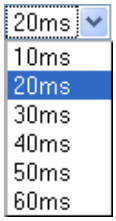
Falls Ihre Upstream-Geschwindigkeit nur 64 kbit/s beträgt, verwenden Sie den Codec G.711 nicht. Für den Codec G.711 sollten mindestens 256 kbit/s für den Upstream zur Verfügung stehen.



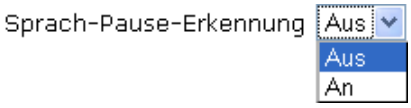
Nur diesen Codec – Wenn dieses Kästchen markiert ist, wird nur der gewählte Codec verwendet.

Paketgröße - Die Datenmenge in einem einzelnen Paket. Der Standardwert ist 20 ms,

d.h. ein Datenpaket enthält 20 ms an Sprachdaten.



Sprach-Pause-Erkennung - Diese Funktion kann erkennen, ob die Sprache auf beiden Seiten aktiv ist oder nicht. Falls nicht, so unternimmt der Router Schritte, um die Bandbreite für andere Zwecke zu sparen. Klicken Sie auf Ein, um diese Funktion zu aktivieren, oder auf Aus, um die Funktion zu deaktivieren.



Nebenstellenrufnummer - Geben Sie eine Nebenstellenrufnummer für das Telefon ein.

E-Mail-Adresse - Geben Sie die E-Mail-Adresse an, an die bei eingehenden Anrufen Mediendateien (Sprachnachrichten) gesendet werden sollen.

Test-eMail versenden: **-** Klicken Sie auf diese Schaltfläche, um eine Test-E-Mail an die eingegebene E-Mail-Adresse zu senden.

Sprachnachricht-Passwort - Geben Sie hier ein Passwort ein. Der Benutzer wird aufgefordert, dieses Passwort einzugeben, um seine Sprachnachrichten anhören zu können.

Anzeige für wartende Nachrichten (MWI) - Falls Sie dieses Kästchen aktivieren, informiert die TK-Anlage den Teilnehmer, wenn im IP-Telefon Sprachnachrichten vorliegen.

Nur wenn TN anfordert - Der Teilnehmer muss zunächst eine Anforderung stellen (SUBSCRIBE). Wenn die TK-Anlage eine neue Sprachmitteilung von einer Nebenstelle entdeckt oder der Zustand der Sprachmitteilung geändert wird, sendet sie innerhalb der gültigen Anforderungszeit eine Nachricht an die entsprechenden Teilnehmer (NOTIFY).

TN immer benachrichtigen - Der Teilnehmer wird benachrichtigt, auch wenn er dies nicht explizit anfordert. Die TK-Anlage benachrichtigt die Teilnehmer, sobald eine neue Nachricht vorliegt oder der Teilnehmer sich erneut an der TK-Anlage anmeldet.

Abgehende Telefonverbindung zulassen - Es stehen für diese Verbindung sechs externe

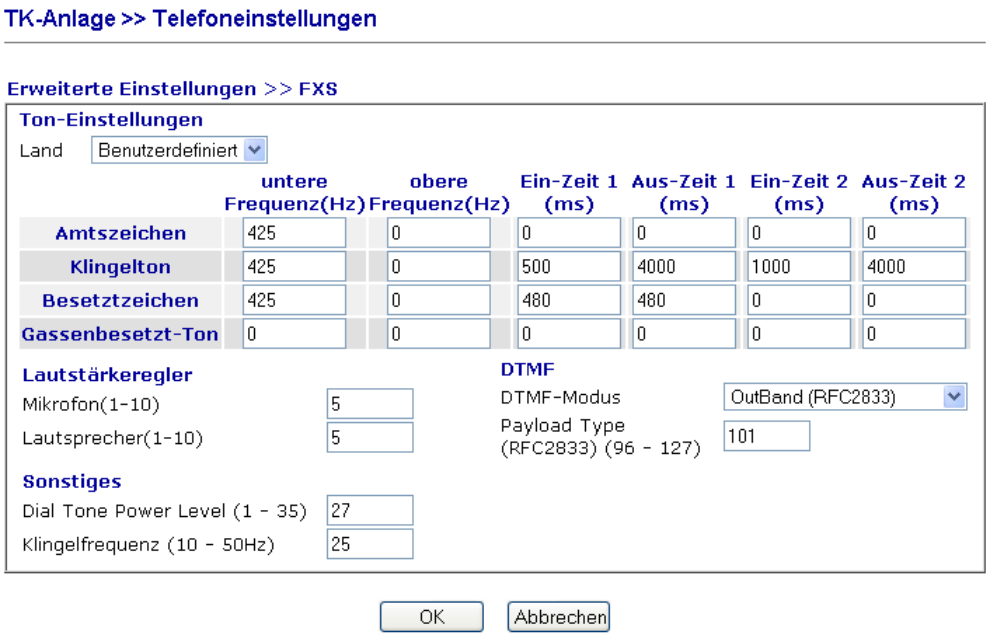
Leitungen und eine ISDN-Leitung zur Verfügung. Bitte markieren Sie die Erwünschte(n).

Anrufbeantwortungsmodus - Geben Sie an, wie mit eingehenden Anrufen umgegangen werden soll.

Wenn keine Antwort nach ….. – Falls ein eingehender Anruf nicht abgenommen wird, kann er gehalten oder zu einer anderen Nebenstelle oder Gruppe umgeleitet werden. Bitte geben Sie die Wartezeit sowie die durchzuführende Aktion an.

Wenn besetzt – Falls diese Nebenstelle besetzt ist, können Sie eingehende Anrufe zu einer anderen Nebenstelle oder Gruppe umleiten.

Zusätzlich können Sie auf **Erweitert** klicken, um Toneinstellungen, Lautstärke, Sonstiges und DTMF-Modus zu konfigurieren. Die Einstellungen unter **Erweitert** ermöglicht die Anpassung des TK-Systems an die örtlichen Gegebenheiten im Umfeld des Routers. Falsche Toneinstellungen können den Teilnehmern unangenehm sein. Um das Tonmuster für den Telefonapparat einzustellen, wählen Sie das richtige Gebiet, um die Voreinstellungen für Ton und Anrufer-ID automatisch durch das System feststellen zu lassen. Um die Toneinstellungen manuell zu konfigurieren, wählen Sie Benutzerdefiniert. TOn1, TOff1, TOn2 und TOff2 beziehen sich auf die Kadenz des Tonmusters. TOn1 und TOn2 stehen für Ton ein, und TOff1 und TOff2 für Ton aus.



Land - Wählen Sie das Land, in dem Sie sich befinden. Die gewöhnlichen Einstellungen für **Anrufer ID-Typ**, **Amtszeichen**, **Klingelton**, **Besetztzeichen** und **Gassenbesetzt-Ton** werden automatisch auf

der Seite angezeigt. Falls Sie keine passenden Einstellungen finden können, wählen Sie bitte **Benutzerdefiniert** und geben die entsprechenden Werte für Amtszeichen, Klingelton, Besetztzeichen und Gassenbesetzt-Ton für das VoIP-Telefon selbst ein.

Sie können jedes Feld nach Bedarf konfigurieren. Wir empfehlen, für die VoIP-Kommunikation die Standardeinstellungen zu verwenden.

LautstärkeMikrofon (1-10)/Lautsprecher (1-10) - Sie können die Lautstärke des Mikrofons und des Lautsprechers durch Eingabe einer Zahl von 1 bis 10 einstellen. Je kleiner die Zahl, desto höher die Lautstärke.

SonstigesLautstärke des Amtszeichens - Diese Einstellung wird verwendet, um die Lautstärke des Amtszeichens einzustellen. Je kleiner die Zahl ist, desto lauter ist das Amtszeichen. Wir empfehlen, die Standardeinstellung zu verwenden.

Klingelfrequenz - Diese Einstellung steuert die Klingelfrequenz. Wir empfehlen, die Standardeinstellung zu verwenden.

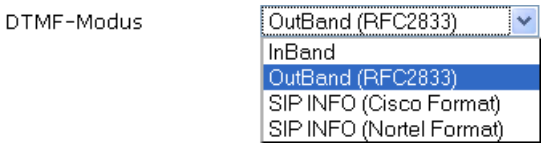
DTMFDTMF-Modus – Es stehen vier DTMF-Modi zur Auswahl.

InBand - Falls Sie diese Einstellung wählen, so sendet der Vigor-Router den DTMF-Ton als Audio, sobald Sie auf die Zifferntaste am Telefon drücken.

OutBand - Falls Sie diese Einstellung wählen, so erfasst der Vigor-Router die gedrückte Zifferntaste, wandelt sie in digital Form um und sendet Sie zur Gegenseite; der Empfänger generiert den Ton gemäß der empfangenen digitalen Form. Diese Funktion ist bei Netzwerkstaus sehr nützlich, da die Genauigkeit des DTMF-Tons erhalten bleibt.

SIP INFO - Falls Sie diese Einstellung wählen, so erfasst der Vigor-Router den

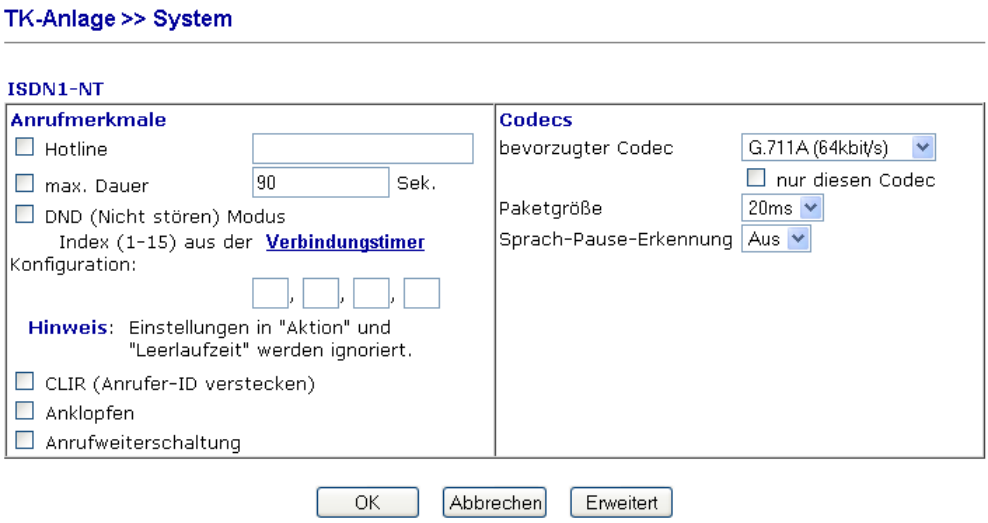
DTMF-Ton und wandelt ihn in SIP-Form um. Dann sendet er ihn per SIP-Nachricht zur entfernten Stelle.



Payload Typ (RFC2833) - Wählen Sie eine Zahl von 96 bis 127; der Standardwert ist 101. Diese Einstellung ist nur für den OutBand (RFC2833) Modus verfügbar.

Erweiterte Einstellungen für ISDN1/2-S0 Port

Klicken Sie auf den Link Index 2 oder Index 3 (ISDN1-S0 oder ISDN2-S0), um zur Konfiguration der Telefoneinstellungen auf die folgende Seite zu gelangen.



Hotline - Markieren Sie das Kästchen, um die Funktion zu aktivieren. Geben Sie die SIP-URL im Feld zur automatischen Wahl ein, wenn Sie den Hörer abnehmen.

Max. Dauer - Markieren Sie dieses Kästchen, um diese Funktion zu aktivieren. Falls innerhalb der in diesem Feld angegebenen Zeit keine Antwort erfolgt, wird der Anruf automatisch geschlossen.

DND (nicht stören) Modus - Hier können Sie eine Ruhezeit eingeben, während der Sie nicht durch VoIP-Anrufe gestört werden möchten. Während dieser Zeit hören die Anrufer das Besetztzeichen, der lokale Teilnehmer hört jedoch keinen Klingelton.

Index (1-15) aus dem Verbindungstimer - Unter den Indexnummern gelangen Sie in die Timerprofile, mit denen Sie den DND-Modus steuern können. Kapitel **5.8.2**

Verbindungstimer enthält Einzelheiten zur Konfiguration.

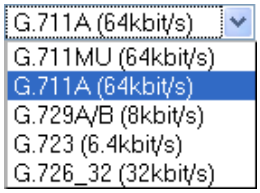
CLIR (Anrufer-ID verstecken) - Markieren Sie dieses Kästchen, um die Anzeige der Anrufer-ID auf dem Display des Telefonapparats zu unterbinden.

Anklopfen - Markieren Sie dieses Kästchen, um diese Funktion zu aktivieren. Ein Hinweiston ertönt, um den Teilnehmer darauf hinzuweisen, dass ein anderer Anruf ansteht. Klicken Sie auf Hook-Flash, um den wartenden Anruf anzunehmen.

Anrufweiterschaltung - Markieren Sie dieses Kästchen, um diese Funktion zu aktivieren. Klicken Sie auf Hook-Flash, um einen anderen Anruf zu tätigen. Falls der Anruf gelingt, legen Sie das Telefon auf. Die anderen beiden Parteien können nun kommunizieren.

Bevorzugter Codec - Hier können Sie einen von fünf Codecs als Standard für Ihre VoIP-Anrufe bestimmen. Der Codec, der für jeden einzelnen Anruf verwendet wird, wird vor jeder Sitzung mit der entfernten Partei ausgehandelt und entspricht eventuell nicht Ihrer Standardwahl. Standardmäßig wird der Codec G.729A/B verwendet, der wenig Bandbreite in Anspruch nimmt aber trotzdem gute Sprachqualität bietet.

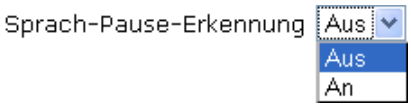
Falls Ihre Upstream-Geschwindigkeit nur 64 kbit/s beträgt, verwenden Sie den Codec G.711 nicht. Für den Codec G.711 sollten mindestens 256 kbit/s für den Upstream zur Verfügung stehen.



Nur diesen Codec – Wenn dieses Kästchen markiert ist, wird nur der gewählte Codec verwendet.

Paketgröße - Die Datenmenge in einem einzelnen Paket. Der Standardwert ist 20 ms, d.h. ein Datenpaket enthält 20 ms an Sprachdaten.

Sprach-Pause-Erkennung - Diese Funktion kann erkennen, ob die Sprache auf beiden Seiten aktiv ist oder nicht. Falls nicht, so unternimmt der Router Schritte, um die Bandbreite für andere Zwecke zu sparen. Klicken Sie auf Ein, um diese Funktion zu aktivieren, oder auf Aus, um die Funktion zu deaktivieren.



Nebenstellenrufnummer - Geben Sie eine Nebenstellenrufnummer für das Telefon ein.

E-Mail-Adresse - Geben Sie die E-Mail-Adresse an, die bei eingehenden Anrufen die Sprachnachrichten gesendet werden sollen.

Test-E-Mail versenden: **-** Klicken Sie auf diese Schaltfläche, um eine Test-E-Mail an die eingegebene E-Mail-Adresse zu senden.

Sprachnachricht-Passwort - Geben Sie hier ein Passwort ein. Der Benutzer wird aufgefordert, dieses Passwort einzugeben, um seine Sprachnachrichten anhören zu können.

Anzeige für wartende Nachrichten (MWI) - Falls Sie dieses Kästchen aktivieren, informiert die TK-Anlage den Teilnehmer, wenn im IP-Telefon Sprachnachrichten vorliegen.

Nur wenn TN anfordert - Der Teilnehmer muss zunächst eine Anforderung stellen (SUBSCRIBE). Wenn die TK-Anlage eine neue Sprachmitteilung von einer Nebenstelle entdeckt oder der Zustand der Sprachmitteilung geändert wird, sendet sie innerhalb der gültigen Anforderungszeit eine Nachricht an die entsprechenden Teilnehmer (NOTIFY).

TN immer benachrichtigen - Der Teilnehmer wird benachrichtigt, auch wenn er dies nicht explizit anfordert. Die TK-Anlage benachrichtigt die Teilnehmer, sobald eine neue Nachricht vorliegt oder der Teilnehmer sich erneut an der TK-Anlage anmeldet.

Max. Dauer - Dies gibt die Dauer an, für welche Ihr SIP-Registrar-Server Ihren Registrierungseintrag aufrecht erhält. Vor Ablauf dieser Zeit sendet der Router erneut eine Registrierungsanforderung an den SIP-Registrar.

Abgehende Telefonverbindung zulassen - Es stehen für diese Verbindung sechs externe Leitungen und eine ISDN-Leitung zur

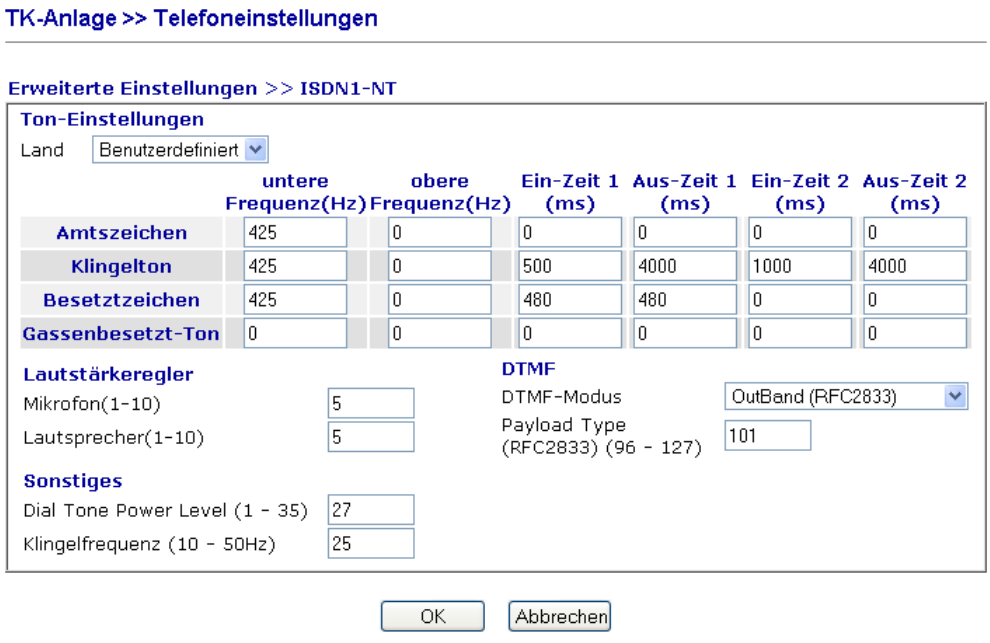
Verfügung. Bitte markieren Sie die gewünschten Verbindungen.

Anrufbeantwortungsmodus - Geben Sie an, wie mit eingehenden Anrufen umgegangen werden soll.

Wenn keine Antwort nach ….. – Falls ein eingehender Anruf nicht abgenommen wird, kann er gehalten oder zu einer anderen Nebenstelle oder Gruppe umgeleitet werden. Bitte geben Sie die Wartezeit sowie die durchzuführende Aktion an.

Wenn besetzt – Falls diese Nebenstelle besetzt ist, können Sie eingehende Anrufe zu einer anderen Nebenstelle oder Gruppe umleiten.

Zusätzlich können Sie auf **Erweitert** klicken, um Toneinstellungen, Lautstärke, Sonstiges, DTMF-Modus und MSN-Nummer zu konfigurieren. Die Einstellungen unter **Erweitert** ermöglicht die Anpassung des TK-Systems an die örtlichen Gegebenheiten im Umfeld des Routers. Falsche Toneinstellungen können den Teilnehmern unangenehm sein. Um das Tonmuster für den Telefonapparat einzustellen, wählen Sie das richtige Gebiet, um die Voreinstellungen für Ton und Anrufer-ID automatisch durch das System feststellen zu lassen. Um die Toneinstellungen manuell zu konfigurieren, wählen Sie Benutzerdefiniert. TOn1, TOff1, TOn2 und TOff2 beziehen sich auf die Kadenz des Tonmusters. TOn1 und TOn2 stehen für Ton ein, und TOff1 und TOff2 für Ton aus.



Land - Wählen Sie das Land, in dem Sie sich befinden. Die gewöhnlichen Einstellungen für **Anrufer ID-Typ**, **Amtszeichen**, **Klingelton**, **Besetztzeichen** und **Gassenbesetzt-Ton -** werden automatisch auf der Seite angezeigt. Falls Sie keine passenden Einstellungen finden können, wählen Sie bitte **Benutzerdefiniert** und geben die entsprechenden Werte für Amtszeichen, Klingelton, Besetztzeichen und

Gassenbesetzt-Ton für das VoIP-Telefon selbst ein.

Sie können jedes Feld nach Bedarf konfigurieren. Wir empfehlen, für die VoIP-Kommunikation die Standardeinstellungen zu verwenden.

LautstärkeMikrofon (1-10)/Lautsprecher (1-10) - Sie können die Lautstärke des Mikrofons und des Lautsprechers durch Eingabe einer Zahl von 1 bis 10 einstellen. Je kleiner die Zahl, desto höher die Lautstärke.

SonstigesLautstärke des Amtszeichens - Diese Einstellung wird verwendet, um die Lautstärke des Amtszeichens einzustellen. Je kleiner die Zahl ist, desto lauter ist das Amtszeichen. Wir empfehlen, die Standardeinstellung zu verwenden.

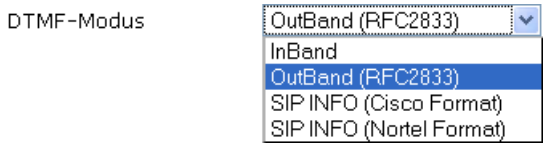
Klingelfrequenz - Diese Einstellung steuert die Klingelfrequenz. Wir empfehlen, die Standardeinstellung zu verwenden.

DTMFDTMF-Modus – Es stehen vier DTMF-Modi zur Auswahl.

InBand - Falls Sie diese Einstellung wählen, so sendet der Vigor-Router den DTMF-Ton als Audio, sobald Sie auf die Zifferntaste am Telefon drücken.

OutBand - Falls Sie diese Einstellung wählen, so erfasst der Vigor-Router die gedrückte Zifferntaste, wandelt sie in digital Form um und sendet Sie zur Gegenseite; der Empfänger generiert den Ton gemäß der empfangenen digitalen Form. Diese Funktion ist bei Netzwerkstaus sehr nützlich, da die Genauigkeit des DTMF-Tons erhalten bleibt.

SIP INFO - Falls Sie diese Einstellung wählen, so erfasst der Vigor-Router den DTMF-Ton und wandelt ihn in SIP-Form um. Dann sendet er ihn per SIP-Nachricht zur entfernten Stelle.

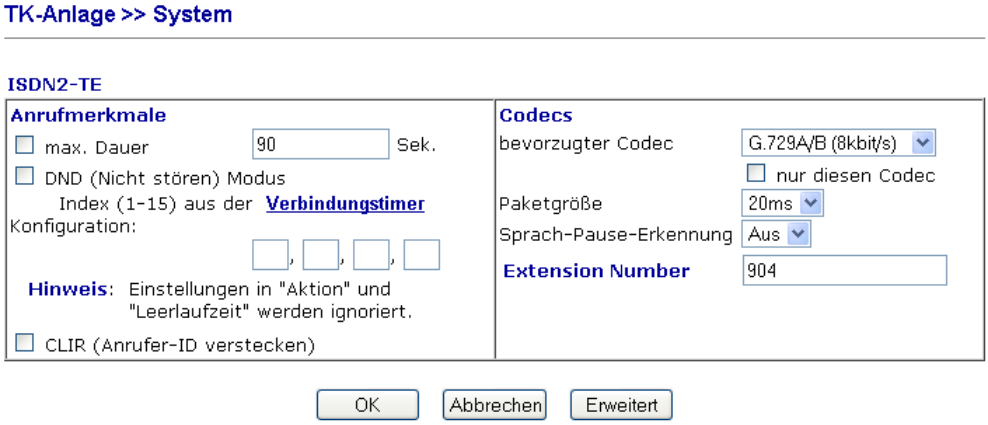


Payload Typ (RFC2833) - Wählen Sie eine Zahl von 96 bis 127; der Standardwert ist 101. Diese Einstellung ist nur für den OutBand (RFC2833) Modus verfügbar.

Erweiterte Einstellungen für ISDN1/2-TE Port

Der Vigor-Router ermöglicht die Umstellung der Funktion des ISDN1/ISDN2-Ports vom TE- auf den S0-Modus. Verwenden Sie die Dropdown-Liste, um den gewünschten Modus zu wählen.

Wenn Sie ISDN-TE wählen und den Link für diesen Port anklicken, erscheint die folgende Seite:



Max. Dauer - Markieren Sie dieses Kästchen, um diese Funktion zu aktivieren. Falls innerhalb der in diesem Feld angegebenen Zeit keine Antwort erfolgt, wird der Anruf automatisch geschlossen.

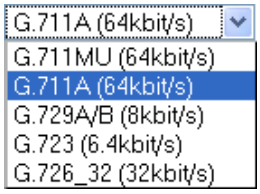
DND (nicht stören) Modus - Hier können Sie eine Ruhezeit eingeben, während der Sie nicht durch VoIP-Anrufe gestört werden möchten. Während dieser Zeit hören die Anrufer das Besetztzeichen, der lokale Teilnehmer hört jedoch keinen Klingelton.

Index (1-15) aus dem Verbindungstimer - Unter den Indexnummern gelangen Sie in die Timerprofile, mit denen Sie den DND-Modus steuern können. Kapitel **5.8.2 Verbindungstimer** enthält Einzelheiten zur Konfiguration.

CLIR (Anrufer-ID verstecken) - Markieren Sie dieses Kästchen, um die Anzeige der Anrufer-ID auf dem Display des Telefonapparats zu unterbinden.

Bevorzugter Codec - Hier können Sie einen von fünf Codecs als Standard für Ihre VoIP-Anrufe bestimmen. Der Codec, der für jeden einzelnen Anruf verwendet wird, wird vor jeder Sitzung mit der entfernten Partei ausgehandelt und entspricht eventuell nicht Ihrer Standardwahl. Standardmäßig wird der Codec G.729A/B verwendet, der wenig Bandbreite in Anspruch nimmt aber trotzdem gute Sprachqualität bietet.

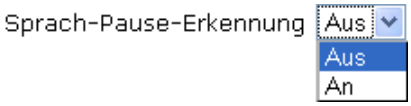
Falls Ihre Upstream-Geschwindigkeit nur 64 kbit/s beträgt, verwenden Sie den Codec G.711 nicht. Für den Codec G.711 sollten mindestens 256 kbit/s für den Upstream zur Verfügung stehen.



Nur diesen Codec – Wenn dieses Kästchen markiert ist, wird nur der gewählte Codec verwendet.

Paketgröße - Die Datenmenge in einem einzelnen Paket. Der Standardwert ist 20 ms, d.h. ein Datenpaket enthält 20 ms an Sprachdaten.

Sprach-Pause-Erkennung - Diese Funktion kann erkennen, ob die Sprache auf beiden Seiten aktiv ist oder nicht. Falls nicht, so unternimmt der Router Schritte, um die Bandbreite für andere Zwecke zu sparen. Klicken Sie auf Ein, um diese Funktion zu aktivieren, oder auf Aus, um die Funktion zu deaktivieren.



Nebenstellenrufnummer - Geben Sie eine Nebenstellenrufnummer für das Telefon ein.

E-Mail-Adresse - Geben Sie die E-Mail-Adresse an, an die bei eingehenden Anrufen Mediendateien (Sprachnachrichten) gesendet werden sollen.

Sprachnachricht-Passwort - Geben Sie hier ein Passwort ein. Der Teilnehmer wird aufgefordert, dieses Passwort einzugeben, um seine Sprachnachrichten anhören zu können.

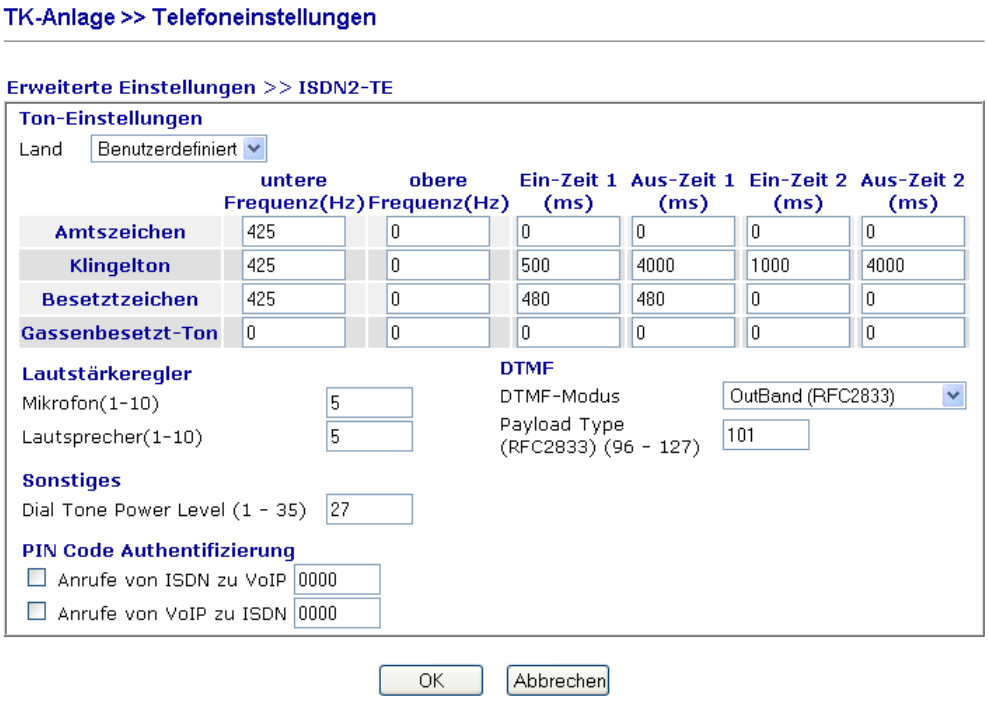
Anzeige für wartende Nachrichten (MWI) Falls Sie dieses Kästchen aktivieren, informiert die TK-Anlage den Teilnehmer, wenn im IP-Telefon Sprachnachrichten vorliegen.

Nur wenn TN anfordert - Der Teilnehmer muss zunächst eine Anforderung stellen (SUBSCRIBE). Wenn die TK-Anlage eine neue Sprachmitteilung von einer Nebenstelle entdeckt oder der Zustand der Sprachmitteilung geändert wird, sendet sie innerhalb der gültigen Anforderungszeit eine Nachricht an die entsprechenden Teilnehmer (NOTIFY).

TN immer benachrichtigen - Der Teilnehmer wird benachrichtigt, auch wenn er dies nicht explizit anfordert. Die TK-Anlage benachrichtigt die Teilnehmer, sobald eine neue Nachricht vorliegt oder der Teilnehmer sich erneut an der TK-Anlage anmeldet.

Max. Dauer - Dies gibt die Dauer an, für welche Ihr SIP-Registrar-Server Ihren Registrierungseintrag aufrecht erhält. Vor Ablauf dieser Zeit sendet der Router erneut eine Registrierungsanforderung an den SIP-Registrar.

Zusätzlich können Sie auf **Erweitert** klicken, um Toneinstellungen, Lautstärke, Sonstiges und DTMF-Modus zu konfigurieren. Die Einstellungen unter **Erweitert** ermöglicht die Anpassung des TK-Systems an die örtlichen Gegebenheiten im Umfeld des Routers. Falsche Toneinstellungen können den Teilnehmern unangenehm sein. Um das Tonmuster für den Telefonapparat einzustellen, wählen Sie das richtige Gebiet, um die Voreinstellungen für Ton und Anrufer-ID automatisch durch das System feststellen zu lassen. Um die Toneinstellungen manuell zu konfigurieren, wählen Sie Benutzerdefiniert. TOn1, TOff1, TOn2 und TOff2 beziehen sich auf die Kadenz des Tonmusters. TOn1 und TOn2 stehen für Ton ein, und TOff1 und TOff2 für Ton aus.



Land - Wählen Sie das Land, in dem Sie sich befinden. Die gewöhnlichen Einstellungen für **Anrufer ID-Typ**, **Amtszeichen**, **Klingelton**, **Besetztzeichen** und **Gassenbesetzt-Ton** werden automatisch auf der Seite angezeigt. Falls Sie keine passenden Einstellungen finden können, wählen Sie bitte **Benutzerdefiniert** und geben die entsprechenden Werte für Amtszeichen, Klingelton, Besetztzeichen und Gassenbesetzt-Ton für das VoIP-Telefon selbst ein.

Sie können jedes Feld nach Bedarf konfigurieren. Wir empfehlen, für die VoIP-Kommunikation die Standardeinstellungen zu verwenden.

LautstärkeMikrofon (1-10)/Lautsprecher (1-10) - Sie können die Lautstärke des Mikrofons und des Lautsprechers durch Eingabe einer Zahl von 1 bis 10 einstellen. Je kleiner die Zahl, desto höher die Lautstärke.

SonstigesLautstärke des Amtszeichens - Diese Einstellung wird verwendet, um die Lautstärke des Amtszeichens einzustellen. Je kleiner die Zahl ist, desto lauter ist das Amtszeichen. Wir empfehlen, die Standardeinstellung zu verwenden.

PIN Code AuthentifizierungAnrufe von ISDN zu VoIP - Setzen Sie einen PIN-Code für den Router zur Authentifizierung bei Anrufen von VoIP zu ISDN. Sie können in diesem Feld einen drei- bis achtstelligen Code bestehend aus den Ziffern 0 bis 9 eingeben.

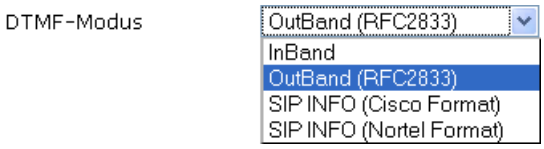
Anrufe von VoIP zu ISDN - Setzen Sie einen PIN-Code für den Router zur Authentifizierung bei Anrufen von VoIP zu ISDN. Sie können in diesem Feld einen drei- bis achtstelligen Code bestehend aus den Ziffern 0 bis 9 eingeben.

DTMFDTMF-Modus – Es stehen hier vier Optionen zur Auswahl:

InBand: - Falls Sie diese Einstellung wählen, so sendet der Vigor-Router den DTMF-Ton als Audio, sobald Sie auf die Zifferntaste am Telefon drücken.

OutBand: - Falls Sie diese Einstellung wählen, so erfasst der Vigor-Router gedrückte Zifferntaste, wandelt sie in digital Form um und sendet Sie zur Gegenseite; der Empfänger generiert den Ton gemäß der empfangenen digitalen Form. Diese Funktion ist bei Netzwerkstaus sehr nützlich, da die Genauigkeit des DTMF-Tons erhalten bleibt.

SIP INFO: - Falls Sie diese Einstellung wählen, so erfasst der Vigor-Router den DTMF-Ton und wandelt ihn in SIP-Form um. Dann sendet er ihn per SIP-Nachricht zur entfernten Stelle.



Payload Typ (RFC2833) - Wählen Sie eine Zahl von 96 bis 127; der Standardwert ist 101. Diese Einstellung ist nur für den OutBand (RFC2833) Modus verfügbar.

5.12.5 Statusanzeige

TK-Anlage >> Statusanzeige

Statusanzeige

Einzelnachweise
Nebenstellen-Monitor

5.12.5.1 Einzelnachweise

Diese Seite zeigt protokollierte TK-Anlagendaten wie fehlgeschlagene Anrufe, erfolgreiche Anrufe, nicht beantwortete Anrufe, Anrufdatum und -dauer usw. an.

TK-Anlage >> Statusanzeige

Einzelnachweise Aktualisierungsintervall (in s): 10 | Aktualisieren |

Index	Datum	Von	Nach	Verbindung	Dauer
1					
2					
3					
4					
5					
6					
44					
45					
46					
47					
48					
49					
50					

<< 1-50 | 51-100 | 101-150 | 151-200 | 201-250 | 251-300 | 301-350 | 351-400 | 401-450 | 451-500
| 501-550 | 551-600 | 601-650 | 651-700 | 701-750 | 751-800 | 801-850 | 851-900 | 901-950 | 951-1000 >>

5.12.5.2 Nebenstellen-Monitor

Diese Seite zeigt den Inhaber, die IP-Adresse, den Status und die Peer-ID jeder Nebenstelle an.

TK-Anlage >> Statusanzeige

Nebenstellen-Monitor Aktualisierungsintervall (in s): 10 | Aktualisieren |

Index	Name	Nebenstellen	IP	Status	Peer ID
1	---	---		Offline	
2	---	---		Offline	
3	---	---		Offline	
4	---	---		Offline	
5	---	---		Offline	
6	---	---		Offline	
7	---	---		Offline	
8	---	---		Offline	
9	---	---		Offline	
10	---	---		Offline	

<< 1-10 | 11-20 | 21-30 | 31-40 | 41-50 >> Weiter >>

5.13 Wireless LAN

Diese Funktion wird nur für das "n"-Modell verwendet.

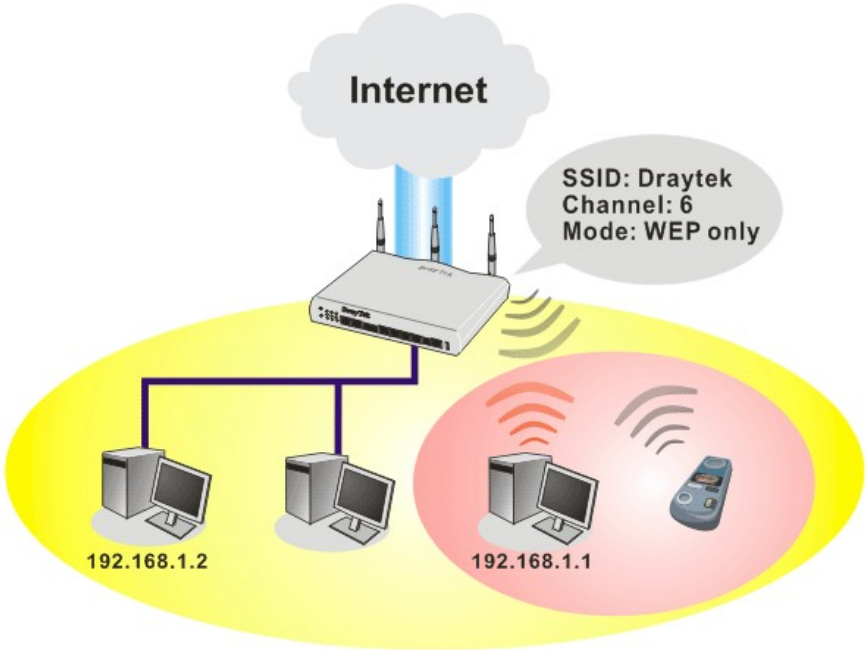
5.13.1 Grundlagen

In den letzten Jahren ist der Markt für kabellose Kommunikation enorm gewachsen. Praktisch jeder Punkt auf der Erde wird mit Wireless-Technologie erreicht oder kann erreicht werden. Viele Menschen tauschen jeden Tag über Wireless-Kommunikationsprodukte Informationen aus. Das Vigor-Modell "n", d.h. der Vigor-Wireless-Router, wurde im Hinblick auf maximale Flexibilität und Effizienz im Kleinunternehmen/Privatbereich konzipiert. Jeder berechtigte Mitarbeiter kann ohne Kabelsalat und Löcher in den Wänden ein WLAN-fähiges PDA oder Notebook im Besprechungszimmer verwenden. Die Mobilität im Wireless LAN ist so hoch entwickelt, dass WLAN-Benutzer gleichzeitig Zugriff auf die gesamte LAN-Ausstattung und auf das Internet haben, genau wie dies bei einem kabelgebundenen LAN der Fall wäre.

Vigor-Wireless-Router sind mit einer WLAN-Schnittstelle ausgerüstet, die dem Standard IEEE 802.11n entspricht. Die fortgeschrittene Wireless-Technologie des Vigor-Routers sorgt für eine weitere Leistungssteigerung, die Übertragungsgeschwindigkeiten von bis zu 300 Mbit/s* ermöglicht. Endlich können Sie nun ruckelfreie Audio- und Videoübertragungen genießen!

Hinweis: * Der tatsächliche Datendurchsatz ändert sich je nach Netzwerkbedingungen und Faktoren wie dem Netzwerkverkehrsvolumen, dem Netzwerk-Overhead und den Objekten in der Umgebung.

In einem Wireless-Netzwerkinfrastrukturmodus dient der Vigor-Wireless-Router als Access Point (AP), mit dem sich verschiedene WLAN-Clients bzw. Stationen (STA) verbinden können. Alle STAs teilen sich den gleichen Internetanschluss über den Wireless-Router. Unter **Basiskonfiguration** werden die Daten zu diesem Wireless-Netzwerk wie die SSID, der Kanal usw. eingestellt.



Verschlüsselungsfunktionen

Echtzeit-Hardware-Verschlüsselung: Der Vigor-Router ist mit einer Hardware-AES-Verschlüsselungs-Engine ausgestattet, um maximalen Schutz der Daten ohne Beeinträchtigung der Nutzung zu ermöglichen.

Umfassende Auswahl von Verschlüsselungsnormen: Um die Sicherheit und die Vertraulichkeit Ihrer Wireless-Kommunikation zu sichern, bieten wir verschiedene marktübliche Normen an.

WEP (Wired Equivalent Privacy) ist eine ältere Methode zur Verschlüsselung jedes per Funk übertragenen Datenpakets mit einem 64- oder 128-Bit-Schlüssel. Normalerweise gibt der Access Point vier Schlüssel vor, wobei nur einer für die Kommunikation mit den einzelnen Clients verwendet wird.

WPA (Wi-Fi Protected Access), der vorherrschende Sicherheitsmechanismus in diesem Sektor, umfasst zwei Kategorien: WPA-Personal, auch bekannt als WPA Pre-Shared Key (WPA/PSK), und WPA-Enterprise, auch bekannt als WPA/802.1x.

Bei WPA-Personal wird während der Datenübertragung ein Pre-Shared Key (vorher vereinbarter Schlüssel) für die Verschlüsselung verwendet. WPA benutzt für die Datenverschlüsselung Temporal Key Integrity Protocol (TKIP), und WPA2 verwendet AES. WPA-Enterprise wird nicht nur für die Verschlüsselung, sondern auch für die Authentifizierung benutzt.

Da sich herausgestellt hat, dass WEP verletzlich ist, ist WPA als sicherste Verbindung zu empfehlen. Wählen Sie Ihren Bedürfnissen entsprechend den geeignetsten Sicherheitsmechanismus. Letztendlich verbessert jede Sicherheitsfunktion den Schutz Ihrer Funkdaten und/oder die Privatsphäre Ihres Wireless-Netzwerks. Der Wireless-Router von Vigor ist sehr flexibel und unterstützt gleichzeitig mehrere sichere Verbindungen mit WEP und WPA.

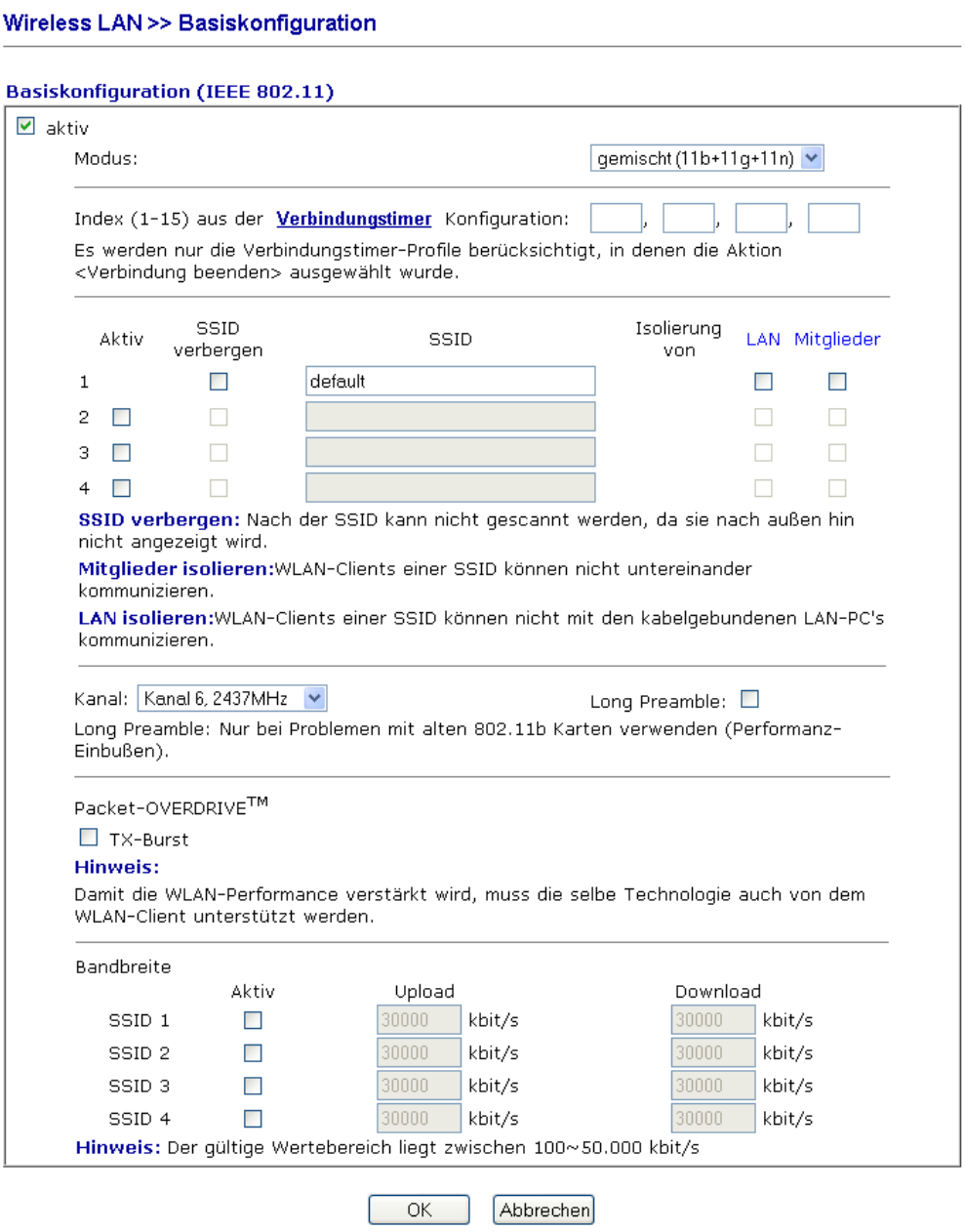
Die **Trennung des Wireless LAN vom kabelgebundenen LAN (WLAN-Isolation)** ermöglicht Ihnen, Ihr Wireless LAN für Quarantäne- oder Zugriffsbeschränkungszwecke vom kabelgebundenen LAN zu isolieren. "Isolieren" bedeutet in diesem Zusammenhang, dass die Parteien keinen Zugriff aufeinander haben. Im geschäftlichen Bereich kann beispielsweise ein Wireless LAN speziell für Besucher eingerichtet werden, so dass diese Zugang zum Internet haben, ohne jedoch auf vertrauliche Daten zugreifen zu können. Weitere Flexibilität kann dadurch erreicht werden, dass MAC-Adressfilter eingesetzt werden, um den Zugriff von Benutzern des kabelgebundenen LANs zu isolieren.

Die **Verwaltung der Wireless Clients (Liste der Clients)** führt alle Clients in Ihrem Wireless-Netzwerk und ihren Verbindungsstatus auf.

Die folgende Abbildung zeigt die Menüeinträge für Wireless LAN an:

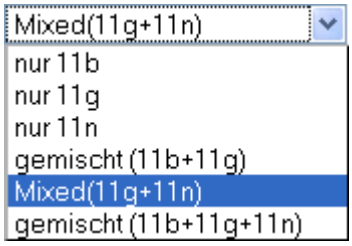
5.13.2 Basiskonfiguration

Wenn Sie auf **Basiskonfiguration** klicken, erscheint eine neue Web-Seite, auf der Sie die SSID und den Wireless-Kanal einstellen können. Die folgende Abbildung enthält weitere Informationen:



Aktiv - Markieren Sie dieses Kästchen, um die Wireless-Funktion zu aktivieren.

Modus - Zur Zeit kann sich der Router über die Modi Nur 11b, Nur 11g, Nur 11n, Gemischt (11b+11g), Gemischt (11g+11n) und Gemischt (11b+11g+11n) mit Clients verbinden. Wählen Sie einfach den Modus Gemischt (11b+11g+11n).



Index (1-15) - Sie können das Wireless LAN so konfigurieren, dass es lediglich in gewissen Zeitabschnitten in Betrieb ist. Sie können bis zu vier der 15 vordefinierten Timer unter **Anwendungen >> Timer** wählen. Per Standardeinstellung ist dieses Feld leer, und die Funktion ist ständig in Betrieb.

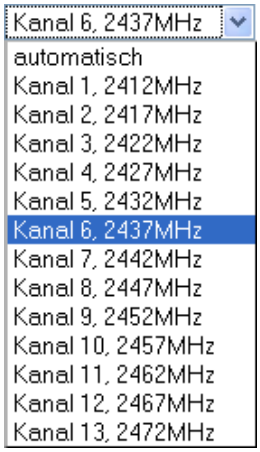
SSID verbergen - Markieren Sie dieses Kästchen, um Wireless-Sniffing zu vermeiden und es für unbefugte Clients oder STAs schwieriger zu machen, sich an Ihrem Wireless LAN anzumelden. Je nach verwendeter Wireless-Technik kann der Benutzer bei der Netzwerksuche lediglich die Information ohne SSID oder überhaupt nichts über den Vigor-Wireless-Router sehen. Das System erlaubt die Eingabe von vier verschiedenen SSIDs für unterschiedliche Zwecke. Standardmäßig wird die erste SSID aktiviert. Sie können diese bei Bedarf verbergen.

SSID - Dies ist die Bezeichnung des Wireless LANs. Die SSID kann aus alphanumerischen Zeichen und Sonderzeichen bestehen. Die Standard-SSID ist "default". Wir empfehlen, diese zu ändern.

Isolierung vonMitglied – Markieren Sie dieses Kästchen, damit Wireless-Clients mit der gleichen SSID keinen gegenseitigen Zugriff haben.

LAN – Markieren Sie dieses Kästchen, damit Wireless-Clients mit der gleichen SSID keinen Zugriff auf kabelgebundene PCs im LAN haben.

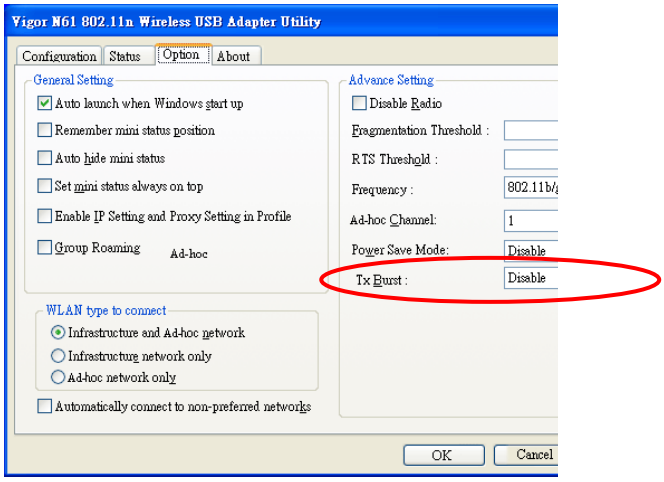
Kanal - Gibt den Frequenzkanal des Wireless LANs an. Der Standardkanal ist 6. Ändern Sie den gewählten Kanal, falls dieser starken Funkstörungen ausgesetzt ist. Falls Sie nicht wissen, welche Frequenz geeignet ist, wählen Sie Auto, um das System die Auswahl treffen zu lassen.



Long Preamble - Diese Option dient der Bestimmung der Länge des Sync-Feldes in einem 802.11-Paket. Die meisten modernen Wireless-Netzwerke verwenden kurze Präambeln mit 56-Bit Sync-Feld anstatt der langen Präambel mit 128-Bit Sync-Feld. Manche originäre 11b Wireless-Netzwerkgeräte unterstützen jedoch nur lange Präambeln. Markieren Sie **Long Preamble**, falls dies erforderlich ist, um mit dieser Art von Geräten zu kommunizieren.

Packet-OVERDRIVE - Durch Markieren von **Tx-Burst** kann die Datenübertragungsleistung bei 11g um ca. 40% verbessert werden (5% bei 11n). Dies ist nur möglich, wenn sowohl der Access Point als auch die Station (im Wireless Client) die Funktion verwenden. Dies bedeutet, dass der Wireless Client diese Funktion sowohl unterstützen als auch aktivieren muss.

Hinweis: - Der Vigor N61 Wireless Adapter unterstützt diese Funktion. Sie können diesen verwenden und in Ihrem Rechner installieren, um die Nutzung von Packet-OVERDRIVE zu ermöglichen (sehen Sie das folgende Bild des Vigor N61 Wireless Konfigurationsfensters; hier muss im Fenster **Optionen** die Funktion **TxBURST** auf **Aktiv** gesetzt werden).



Bandbreite - Legt die Datenübertragungsgeschwindigkeit über die kabellose Verbindung fest.

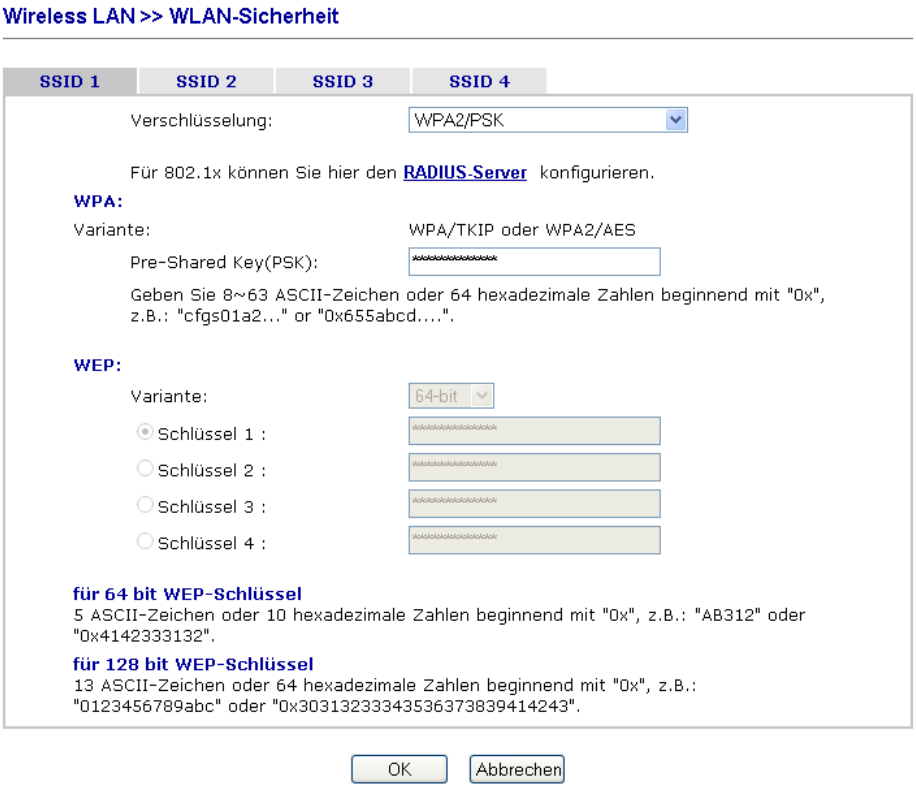
Upload – Klicken Sie auf **Aktiv** und geben Sie die Übertragungsgeschwindigkeit für Uploads an. Der Standardwert beträgt 30.000 kbps.

Download – Geben Sie die Übertragungsgeschwindigkeit für Downloads an. Der Standardwert beträgt 30.000 kbps.

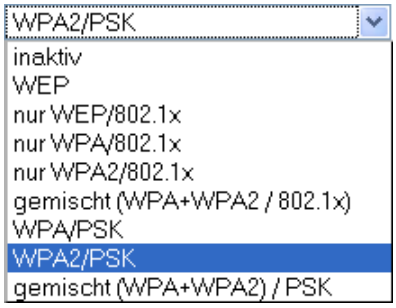
5.13.3 Verschlüsselung

Diese Seite ermöglicht Ihnen die Konfiguration der Sicherheit mit verschiedenen Modi für SSID 1, 2, 3 und 4. Nach Abschluss der Konfiguration klicken Sie bitte auf **OK**, um die Einstellungen zu speichern und anzuwenden.

Wenn Sie auf **Verschlüsselung** klicken, erscheint eine neue Web-Seite, auf der Sie die WEP- und WPA-Einstellungen konfigurieren können.



Modus - Es stehen verschiedene Modi zur Auswahl.



Inaktiv - Verschlüsselung abschalten.

WEP - Akzeptiert nur WEP-Clients; der Schlüssel für die Verschlüsselung muss unter WEP-Schlüssel eingetragen werden.

Nur WEP/802.1x - Nimmt nur WEP-Clients an; der Verschlüsselungsschlüssel wird über das 802.1X-Protokoll dynamisch vom RADIUS-Server bezogen.

Nur WPA/802.1x - Nimmt nur WPA-Clients an; der Verschlüsselungsschlüssel wird über das 802.1X-Protokoll dynamisch vom RADIUS-Server bezogen.

Nur WPA2/802.1x - Nimmt nur WPA2-Clients an; der Verschlüsselungsschlüssel wird über das 802.1X-Protokoll dynamisch vom RADIUS-Server bezogen.

Gemischt (nur WPA+WPA2/802.1x) - Akzeptiert nur WPA- und WPA2-Clients gleichzeitig; der Schlüssel für die Verschlüsselung wird über das 802.1X-Protokoll dynamisch vom RADIUS-Server bezogen.

WPA/PSK - Akzeptiert nur WPA-Clients; der Schlüssel für die Verschlüsselung muss unter PSK eingeben werden.

WPA2/PSK -Akzeptiert nur WPA2-Clients; der Schlüssel für die Verschlüsselung muss unter PSK eingegeben werden.

Gemischt (WPA+ WPA2)/PSK - Akzeptiert gleichzeitig WPA- und WPA2-Clients; der Schlüssel für die Verschlüsselung muss unter PSK eingegeben werden.

Hinweis: Bei Auswahl von **Nur WEP/802.1x**, **Nur WPA/802.1x**, **Nur WPA2/802.1x** oder **Gemischt (WPA+WPA2/802.1x)** sollten Sie gleichzeitig den RADIUS-Server aktivieren.

WPA - WPA verschlüsselt jedes per Funk übertragene Paket entweder mit dem PSK (Pre-Shared Key), der in dem Feld unten manuell

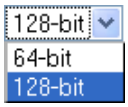
eingegeben wurde, oder mit dem automatisch per 802.1x-Authentifizierung verhandelten Schlüssel. Hierzu werden entweder **8~63** ASCII-Zeichen, z.B. "012345678..." oder 64 hexadezimale Ziffern, angeführt von "0x", z.B. "0x321253abcde..." verwendet.

Typ - Auswahl zwischen Gemischt (WPA+WPA2) oder Nur WPA2.

Pre-Shared Key (PSK) - Entweder **8~63** ASCII-Zeichen, z.B. "012345678..." oder 64 hexadezimale Zeichen, angeführt von "0x", z.B. "0x321253abcde...".

WEP64-Bit - Für 64-Bit WEP-Schlüssel; entweder **5** ASCII-Zeichen, z.B. "12345", oder 10 hexadezimale Ziffern, angeführt von "0x", z.B. "0x4142434445".

128-Bit - Für 128-Bit WEP-Schlüssel; entweder **13** ASCII-Zeichen, z.B. "ABCDEFGHIJKLM", oder 26 hexadezimale Ziffern, angeführt von "0x", z.B. "0x41424344454647484 94A4B4C4D".



Alle Wireless-Geräte müssen die gleiche WEP-Verschlüsselungslänge unterstützen und den gleichen Schlüssel verwenden. Hier können **vier Schlüssel** eingegeben werden, aber es kann jeweils nur ein Schlüssel ausgewählt werden. Die Schlüssel können in ASCII oder hexadezimal eingegeben werden. Haken Sie den Schlüssel an, den Sie verwenden möchten.

5.13.4 Zugriffskontrolle

Um den Wireless-Zugriff zusätzlich abzusichern, ermöglicht Ihnen die **Zugriffskontrolle**, den Zugriff auf das Netzwerk über die Wireless LAN MAC-Adresse des Clients zu steuern. So wird nur gültigen MAC-Adressen erlaubt, auf die Wireless LAN Schnittstelle zuzugreifen. Wenn Sie auf **Zugriffskontrolle** klicken, erscheint eine neue Web-Seite wie unten abgebildet, in der Sie die MAC-Adressen der Clients bearbeiten können, um deren Zugriffsrechte zu steuern.

MAC-Whitelist - Hier kann der MAC-Adressenfilter für das Wireless LAN für SSID 1 bis 4 aktiviert werden. Alle im Feld aufgeführten Clients (ausgedrückt durch MAC-Adressen) können in verschiedene Wireless LANs gruppiert werden. Falls Sie beispielsweise SSID 1 und SSID 2 markieren, können sie gleichzeitig unter SSID 1 und SSID 2 gruppiert werden.

MAC-Adressenfilter - Alle MAC-Adressen anzeigen, die zuvor bearbeitet wurden.

MAC-Adresse des Clients - Geben Sie die MAC-Adresse des Wireless-Clients manuell ein.

Attributs: Client vom LAN isolieren - Markieren, um die Wireless-Verbindung des Wireless-Clients mit der MAC-Adresse vom LAN zu trennen.

Hinzufügen - Der Liste eine neue MAC-Adresse hinzufügen.

Löschen - Ausgewählte MAC-Adresse aus der Liste löschen.

Bearbeiten - Ausgewählte MAC-Adresse in der Liste bearbeiten.

Abbrechen - Konfiguration der Zugriffskontrolle abbrechen.

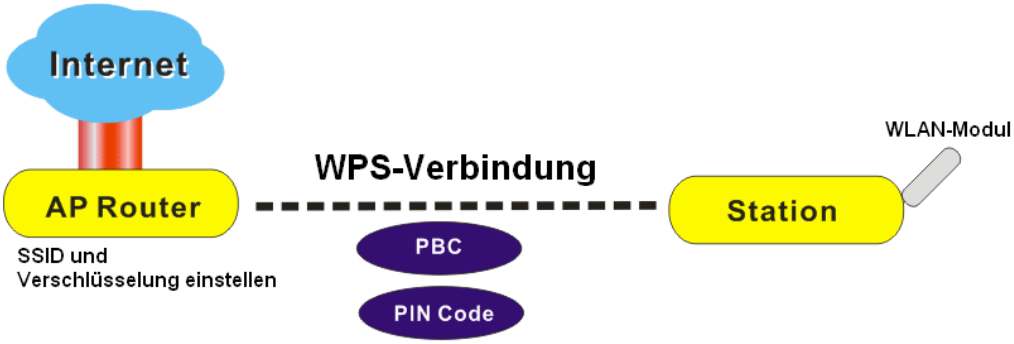
OK - ACL speichern.

Alle löschen - Alle Einträge in der MAC-Adressenliste löschen.

Alle löschen - Alle Einträge in der MAC-Adressenliste löschen.

5.13.5 WPS

WPS (Wi-Fi Protected Setup) ist eine einfache Methode, um WPA- und WPA2-verschlüsselte Netzwerkverbindungen zwischen WLAN-Clients und dem Wireless Access Point (Vigor-Router) aufzubauen.

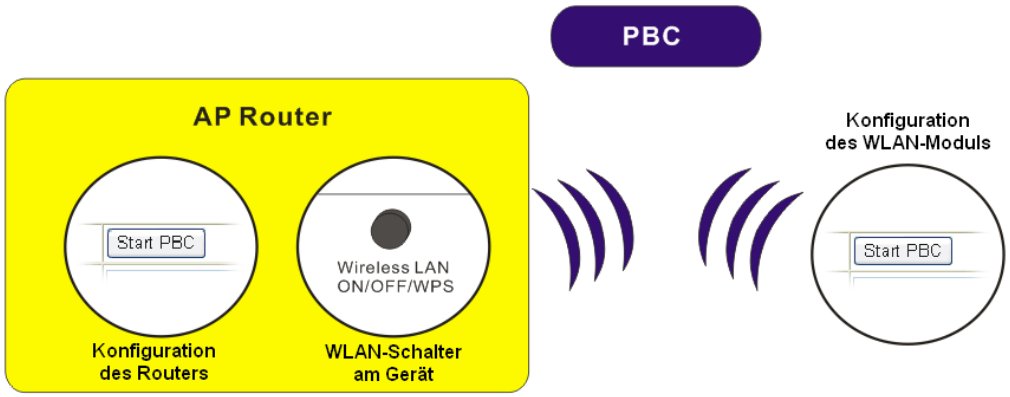


Hinweis: Diese Funktion ist nur für WLAN-Clients verfügbar, die WPS unterstützen.

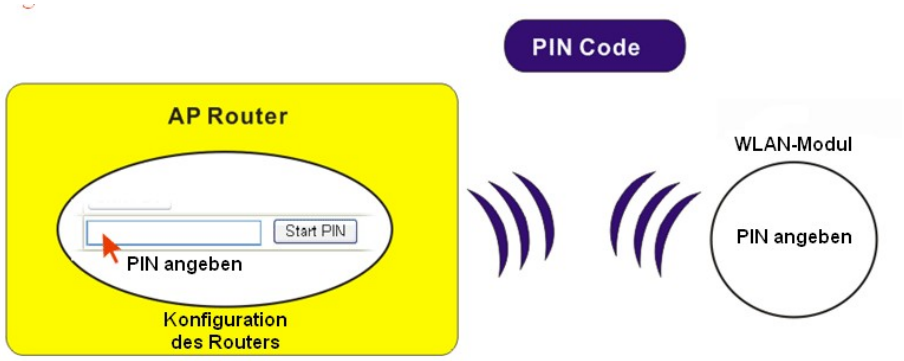
Dies ist der einfachste Ansatz zum Aufbau einer Verbindung zwischen WLAN-Clients und dem Vigor-Router. Benutzer brauchen nicht jedes Mal den Verschlüsselungsmodus zu wählen und ein langes Verschlüsselungspasswort einzugeben, um einen WLAN-Client einzurichten. Es genügt, die **WPS**-Taste am AP zu betätigen und den AP im Menü des Clients zu wählen, um die Verbindung des Clients und des Routers automatisch über WPS aufzubauen.

Die Netzwerkverbindung über WPS zwischen dem AP und den Clients kann in zweierlei Weise aufgebaut werden: Durch Drücken auf ***Starte PBC*** oder durch Eingabe des ***PIN-Codes***.

- Auf der Seite der als AP verwendeten VigorIPPBX 2820-Serie halten Sie die Taste **Wireless LAN EIN/AUS/WPS** zwei Sekunden lang gedrückt, damit das Client-Gerät die Netzwerkverbindung über WPS aufbaut, oder klicken Sie auf **Starte PBC** im Konfigurationsmenü. Auf dem Client, auf dem die Netzwerkkarte installiert ist, drücken Sie auf **Starte PBC** der Netzwerkkarte.



- Um den PIN-Code zu benutzen, müssen Sie den im WLAN-Client angegebenen PIN-Code kennen. Geben Sie den PIN-Code des mit dem Vigor-Router zu verbindenden WLAN-Clients ein.



-

Da WPS entweder WPA-PSK oder WPA2-PSK erfordert, wird die folgende Meldung angezeigt, falls Sie nicht in **Wireless LAN>>Verschlüsselung** einen dieser Modi wählen.

Klicken Sie auf **OK** und gehen Sie zurück zu **Wireless LAN>>Verschlüsselung**, um WPA-PSK oder WPA2-PSK zu wählen, und starten Sie WPS erneut.

Web-Seite für **Wireless LAN>>WPS**:

Aktiv - Markieren Sie dieses Kästchen, um WPS zu aktivieren.

WPS-Status - Zeigt WPS-bezogene Systeminformationen an.

SSID - SSID1 des Routers anzeigen. WPS wird nur von SSID1 unterstützt.

Authentifizierungs-Modus - Aktuellen Authentifizierungs-Modus des Routers anzeigen. Nur WPA2/PSK und WPA/PSK unterstützen WPS.

Konfiguration per Knopfdruck (PBC) - Klicken Sie auf **Starte PBC**, um die WPS-Einrichtung per Knopfdruck zu starten. Der Router wartet ca. zwei Minuten auf WPS-Anfragen von WLAN-Clients. Während WPS in Betrieb ist, blinkt die WPS-LED am Router schnell. Die LED kehrt nach zwei Minuten in den Normalzustand zurück (d.h. WPS muss innerhalb von zwei Minuten eingerichtet werden).

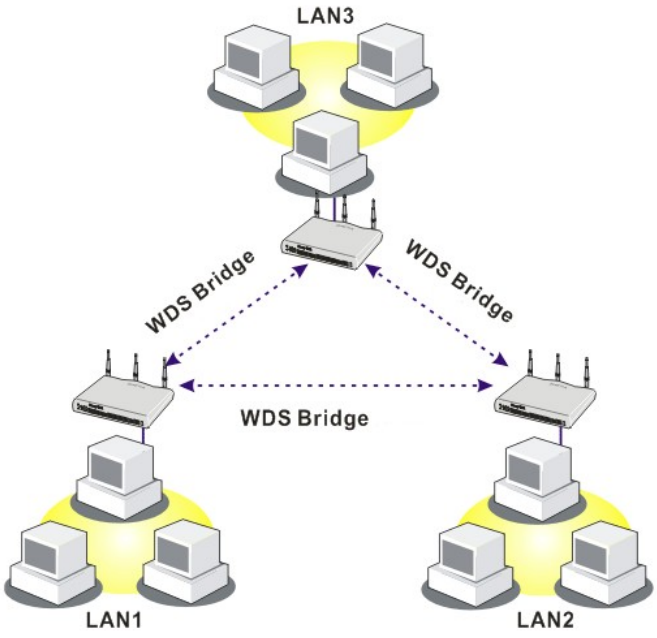
Konfiguration via PIN-Code - Geben Sie den PIN-Code des zu verbindenden WLAN-Clients ein und klicken Sie auf **Start-PIN**. Während WPS in Betrieb ist, blinkt die WPS-LED am Router schnell. Die LED kehrt nach zwei Minuten in den Normalzustand zurück (d.h. WPS muss innerhalb von zwei Minuten eingerichtet werden).

5.13.6 WDS

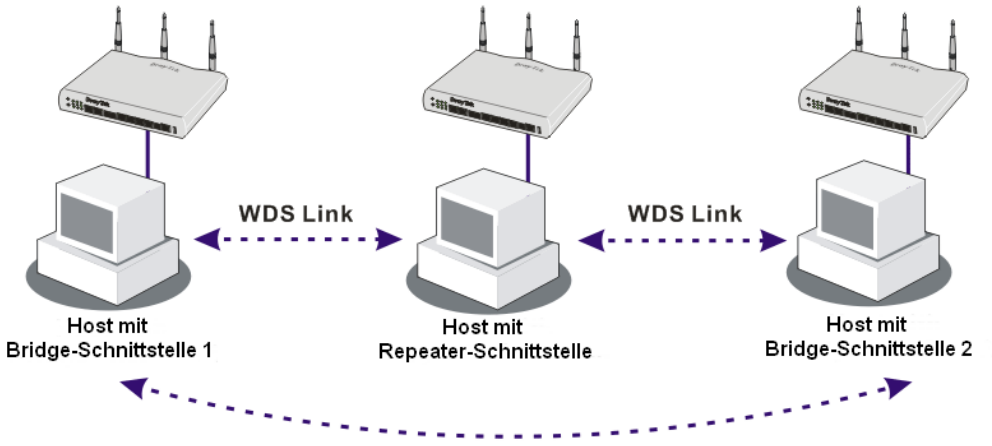
WDS ist die Abkürzung für Wireless Distribution System. Es handelt sich hierbei um ein Protokoll zur drahtlosen Verbindung von zwei Access Points (AP). Üblicherweise wird diese Technik für die folgenden Zwecke eingesetzt:

- Drahtlose Überbrückung zweier LANs.
- Erweiterte Reichweite eines WLANs.

Um diese Anforderungen zu erfüllen, bietet der Vigor-Router zwei WDS-Modi: **Bridge** und **Repeater**. Die folgende Abbildung zeigt die Funktionsweise der WDS-Bridge-Schnittstelle:

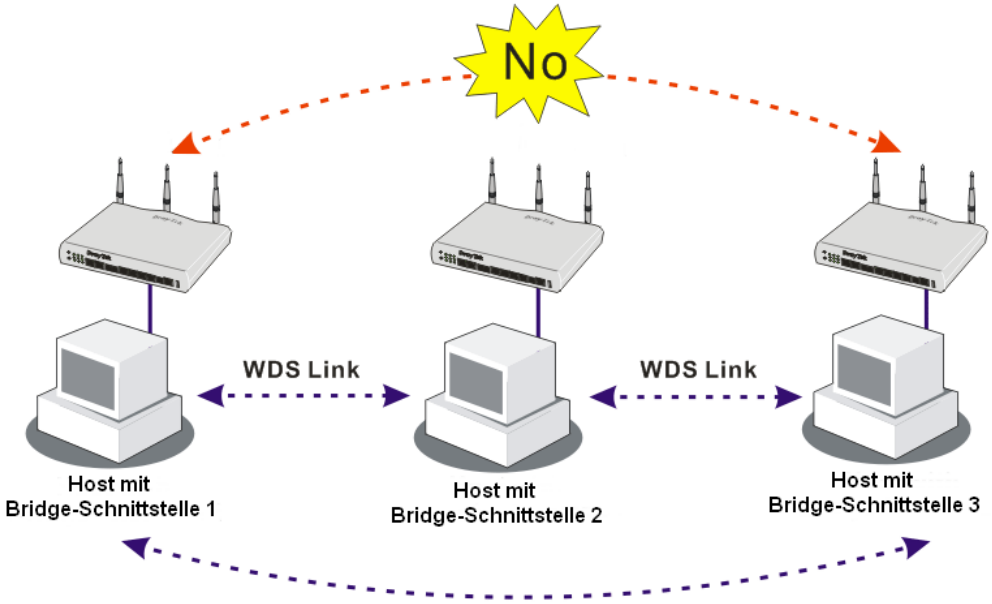


Die WDS-Repeater-Anwendung funktioniert wie folgt:

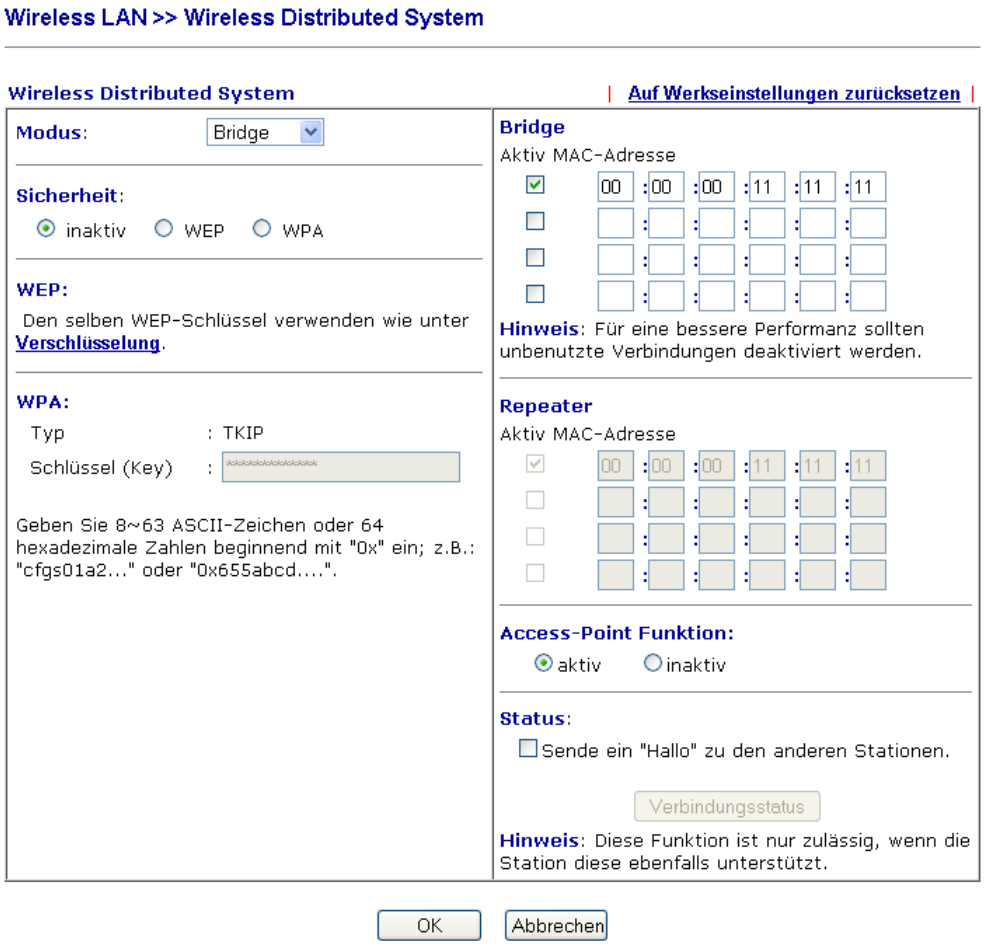


Der Hauptunterschied zwischen diesen beiden Modi ist wie folgt: Im **Repeater**-Modus werden die von einem Peer-AP empfangenen Pakete über WDS-Verbindungen an andere Peer-APs wiederholt. Im **Bridge**-Modus hingegen werden Pakete, die über eine WDS-Verbindung empfangen wurden, lediglich an lokale kabelgebundene oder Wireless-Hosts weitergeleitet. Anders ausgedrückt ist nur der Repeater-Modus in der Lage, Pakete von WDS zu WDS zu übertragen.

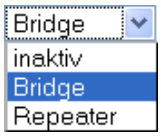
In den folgenden Beispielen können mit Bridge 1 oder 3 verbundene Hosts über WDS-Verbindungen mit Hosts kommunizieren, die mit Bridge 2 verbunden sind. Hosts, die mit Bridge 1 verbunden sind, können jedoch NICHT mit Hosts kommunizieren, die über Bridge 2 mit Bridge 3 verbunden sind.



Klicken Sie im Menü **Wireless LAN** auf **WDS**. Die folgende Seite erscheint.



Modus - Wählen Sie den Modus für die WDS-Einstellungen. **Inaktiv** bedeutet, dass keine WDS-Einstellungen verwendet werden. Der **Bridge**-Modus dient dem ersten Anwendungsfall. Der **Repeater**-Modus dient dem zweiten Anwendungsfall.



Verschlüsselung - Es stehen drei Optionen zur Auswahl: **Inaktiv**, **WEP** und **Pre-Shared Key**. Die hier gewählte Einstellung bestimmt, ob das folgende WEP oder Pre-Shared Key Feld zutrifft oder nicht. Wählen Sie einen der Typen für den Router.

WEP - Markieren Sie dieses Kästchen, um den gleichen Schlüssel zu verwenden, der auf der Seite **Verschlüsselung** gesetzt wurde. Falls auf der Seite **Verschlüsselung** kein Schlüssel gesetzt wurde, ist dieses Kästchen inaktiv.

Pre-Shared KeyTyp – Es stehen drei Typen zur Auswahl. **DrayTek WPA** kann für sämtliche DrayTek Wireless-Router wie Vigor2700, Vigor2800, Vigor2820 usw.

verwendet werden, nicht jedoch für die Wireless-Router anderer Hersteller. **WPA** und **WPA2** werden für WDS-Geräte verwendet (z.B. AP700). Falls Sie beispielsweise einen Wireless-AP und einen Vigor2820n Wireless-Router betreiben, können Sie den Verschlüsselungsmodus auf WPA oder WPA2 setzen, um Ihr WDS-System zwischen dem AP und dem Router aufzusetzen.

Schlüssel - Geben Sie 8 ~ 63 ASCII-Zeichen 64 hexadezimale Ziffern, angeführt von "0x", ein.

Bridge - Falls Sie als Verbindungsmodus Bridge wählen, geben Sie bitte die MAC-Adresse der Peers in diesen Feldern ein. Es können bis zu vier MAC-Adressen von Peers gleichzeitig eingegeben werden. Bitte deaktivieren Sie jedoch unbenutzte Verbindungen, um die Leistung zu verbessern. Markieren Sie nach der Eingabe das Kästchen **Aktiv** vor der MAC-Adresse, um die entsprechende MAC-Adresse zu aktivieren.

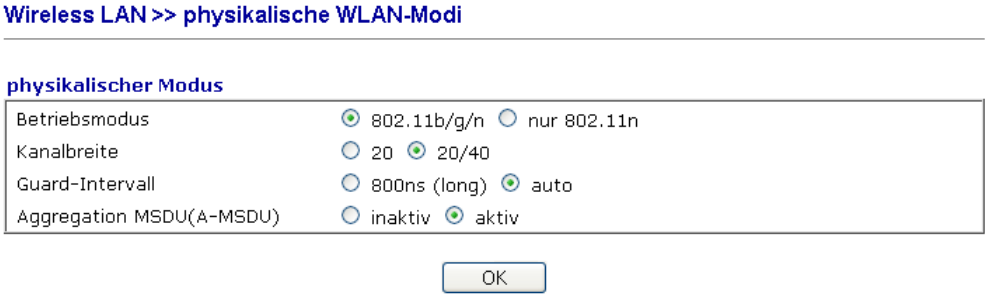
Repeater - Falls Sie als Verbindungsmodus Repeater wählen, geben Sie bitte die MAC-Adresse der Peers in diesen Feldern ein. Es können bis zu vier MAC-Adressen von Peers gleichzeitig eingegeben werden. Markieren Sie nach der Eingabe das Kästchen **Aktiv** vor der MAC-Adresse, um die entsprechende MAC-Adresse zu aktivieren.

Access-Point Funktion - Klicken Sie auf **Aktiv**, um diesen Router als Access Point zu verwenden; klicken Sie auf **Inaktiv**, um diese Funktion auszuschalten.

Status - Hiermit können den Peers "hello"-Meldungen geschickt werden, vorausgesetzt, die Peers unterstützen diese Funktion.

5.13.7 Erweiterte Einstellungen

Diese Seite ermöglicht die Konfiguration von erweiterten Einstellungen wie Betriebsmodus, Kanalbreite, Guard-Intervall und Aggregation MSDU für kabellose Datenübertragung.



Betriebsmodus802.11b/g/n – Der Router kann Daten über 802.11b/g/n übermitteln. Die gesamte Drahtlosübertragung verlangsamt sich jedoch, falls Wireless-Clients mit 802.11g oder 802.11b angebunden werden.

Nur 802.11n – Wählen Sie diesen Modus, um den Durchsatz zu maximieren. In diesem Modus ist die Datenübertragung nur zwischen 11n-Systemen möglich. Außerdem besteht kein Mechanismus zum Schutz vor Konflikten mit anliegenden 802.11a/b/g-Geräten.

Kanalbreite20 – Der Router verwendet 20 MHz zum Senden und Empfangen von Daten zwischen dem AP und den Clients.

20/40 – Der Router verwendet je nach Kapazität des Clients 20 oder 40 MHz zum Senden und Empfangen. Diese Kanalbreite kann die Datendurchgangsleistung verbessern.

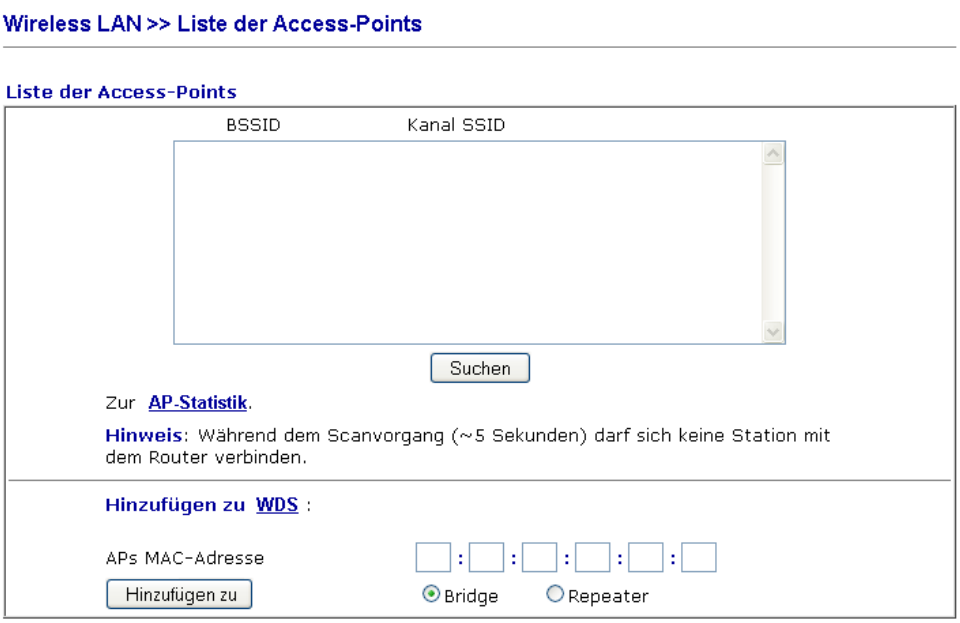
Guard-Intervall - Schützt empfindliche digitale Daten vor Ausbreitungsverzögerungen und Reflexionen. Falls Sie **Automatisch** als Guard-Intervall wählen, verwendet der AP-Router je nach Fähigkeit der Clients entweder kurze Guard-Intervalle (um die Wireless-Leistung zu verbessern) oder lange Guard-Intervalle für die Datenübertragung.

Aggregation MSDU - Aggregation MSDU kann Datenpakete verschiedener Größen kombinieren. Diese Funktion verbessert die Leistung des MAC-Layers für Clients einiger Hersteller. Die Standardeinstellung ist **Aktiv**.

5.13.8 Liste der Access Points

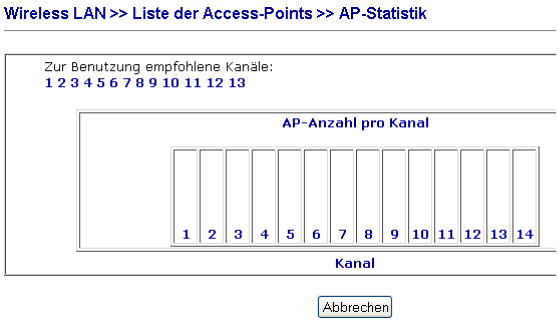
Vigor-Router können alle Standardkanäle scannen und in Betrieb befindliche APs in der Umgebung auffinden. Aufgrund des Suchergebnisses erfahren Benutzer, welcher Kanal zur Benutzung geeignet ist. Diese Funktion kann auch zur Suche nach einem AP für eine WDS-Verbindung genutzt werden. Beachten Sie, dass sich kein Client während des Suchprozesses (ca. 5 Sekunden) mit dem Vigor-Router verbinden kann.

Diese Seite wird zur Suche von APs im Wireless LAN verwendet. Es werden jedoch nur APs erkannt, die sich auf dem gleichen Kanal befinden, wie dieser Router. Klicken Sie auf **Suchen**, um alle verbundenen APs zu erkennen.



Suchen - Sucht nach allen verbundenen APs. Die Ergebnisse werden im Feld über dieser Taste angezeigt.

Statistik - Zeigt die Statistik der von APs benutzten Kanäle an.


Wireless LAN >> Liste der Access-Points >> AP-Statistik
Zur Benutzung empfohlene Kanäle:
1 2 3 4 5 6 7 8 9 10 11 12 13
AP-Anzahl pro Kanal
1 2 3 4 5 6 7 8 9 10 11 12 13 14
Kanal
Abbrechen

Hinzufügen zu - Falls Sie einen gefundenen AP zur WDS-Konfiguration hinzufügen möchten, geben Sie bitte die MAC-Adresse des APs unten auf der Seite ein oder wählen die AP MAC-Adresse aus dem Feld mit dem Suchergebnis und klicken auf **Bridge** oder **Repeater**. Dann klicken Sie auf **Hinzufügen zu**. Die MAC-Adresse des APs wird dem Bridge- oder Repeater-Feld auf der WDS-Konfigurationsseite hinzugefügt.

5.13.9 Liste der Clients

Die **Liste der Clients** enthält Informationen über die aktuell verbundenen Clients und den Status-Code. Die Codes werden unten erläutert. Zwecks **Zugriffskontrolle** können Sie einen WLAN-Client wählen und auf **Hinzufügen** klicken.

Aktualisieren - Klicken Sie auf diese Taste, um den Status der Client-Liste zu aktualisieren.

Hinzufügen - Klicken Sie auf diese Taste, um die aktuell gewählte MAC-Adresse der **Zugriffskontrolle** hinzuzufügen.

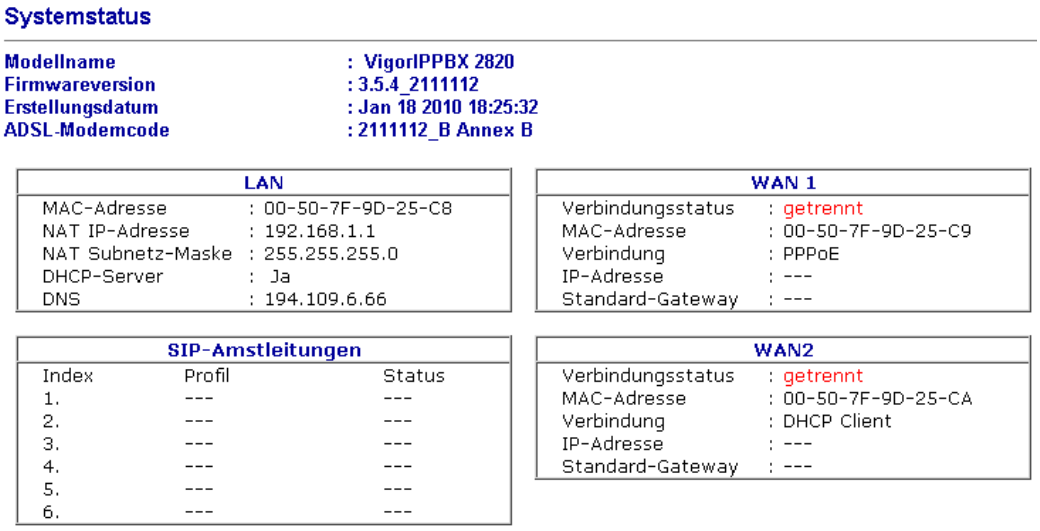
5.14 Systemmanagement

Es gibt verschiedene Bereiche, die für die Konfiguration von Bedeutung sind: Status, Administratorpasswort, Konfigurations-Backup, Syslog, Zeit und Datum, Neustart und Aktualisierung der Firmware.

Die folgende Abbildung zeigt die Menüeinträge für das Systemmanagement:

5.14.1 Systemstatus

Im **Systemstatus** sehen Sie grundlegende Netzwerkeinstellungen des Vigor-Routers. Dies umfasst Informationen über die LAN- und WAN-Schnittstellen. Außerdem werden die aktuelle Version und Informationen bezüglich dieser Firmware angezeigt.



Systemstatus

Modellname	: VigorIPPBX 2820
Firmwareversion	: 3.5.4_2111112
Erstellungsdatum	: Jan 18 2010 18:25:32
ADSL-Modemcode	: 2111112_B Annex B

LAN	
MAC-Adresse	: 00-50-7F-9D-25-C8
NAT IP-Adresse	: 192.168.1.1
NAT Subnetz-Maske	: 255.255.255.0
DHCP-Server	: Ja
DNS	: 194.109.6.66

WAN 1	
Verbindungsstatus	: getrennt
MAC-Adresse	: 00-50-7F-9D-25-C9
Verbindung	: PPPoE
IP-Adresse	: ---
Standard-Gateway	: ---

SIP-Amstleitungen		
Index	Profil	Status
1.	---	---
2.	---	---
3.	---	---
4.	---	---
5.	---	---
6.	---	---

WAN2	
Verbindungsstatus	: getrennt
MAC-Adresse	: 00-50-7F-9D-25-CA
Verbindung	: DHCP Client
IP-Adresse	: ---
Standard-Gateway	: ---

Modellname - Modellname des Routers

Firmwareversion - Firmwareversion des Routers

Erstellungsdatum - Datum und Uhrzeit der Erstellung der aktuellen Firmware

ADSL-Modemcode - ADSL-Firmwareversion

LAN-------

MAC-Adresse - MAC-Adresse der LAN-Schnittstelle

NAT IP-Adresse - IP-Adresse der LAN-Schnittstelle

Subnetz-Maske - Adresse der Subnetz-Maske der LAN-Schnittstelle

DHCP-Server - Aktueller Status des DHCP-Servers der LAN-Schnittstelle

DNSZugewiesene IP-Adresse des bevorzugten DNS-Servers

WAN-------

Verbindungsstatus - Aktueller Verbindungsstatus

MAC-Adresse - MAC-Adresse der WAN-Schnittstelle

Verbindung - Verbindungsart

IP-Adresse - IP-Adresse der WAN-Schnittstelle

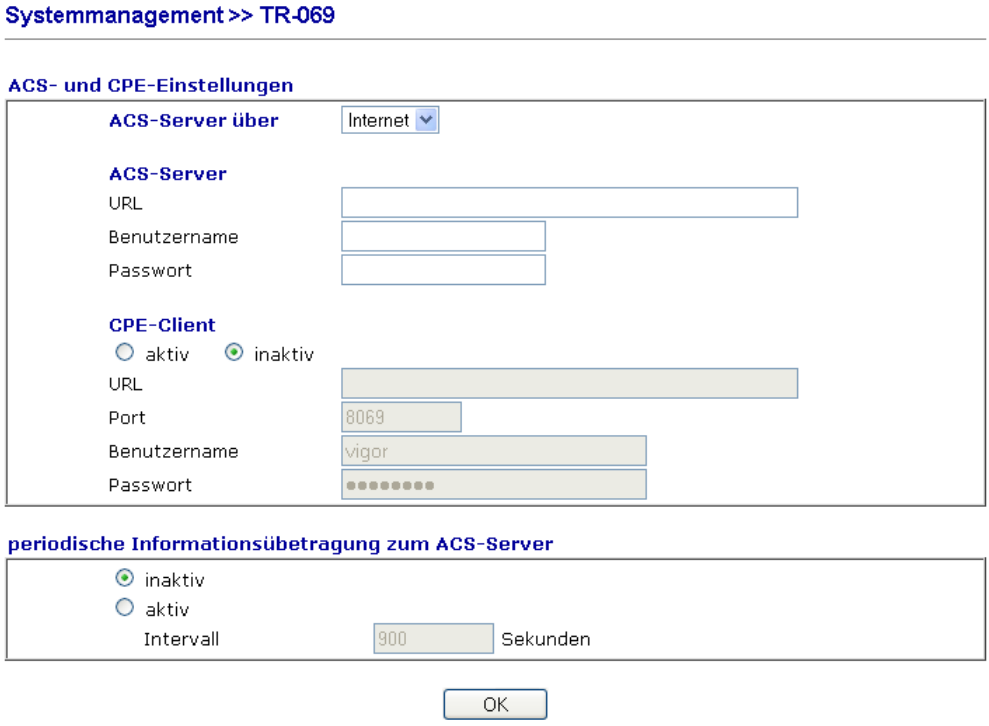
Standard-Gateway - Zugewiesene IP-Adresse des Standard-Gateways

SIP-Amtsleitung-------

Index/Profil/Status - Aktueller Status der SIP-Profile.

5.14.2 TR-069

Dieses Gerät unterstützt die Norm TR-069. Es ist für einen Administrator sehr bequem, ein TR-069-Gerät über einen Auto-Konfigurationsserver wie VigorACS zu verwalten.



ACS-Server über - Wählen Sie die Schnittstelle, über die der Router mit dem ACS-Server verbunden werden soll.

ACS-ServerURL/Benutzername/Passwort – Diese Daten müssen für den ACS (Auto Configuration Server) eingegeben werden, zu dem Sie eine Verbindung aufbauen möchten. Weitere Einzelheiten sind im Benutzerhandbuch des ACS verfügbar.

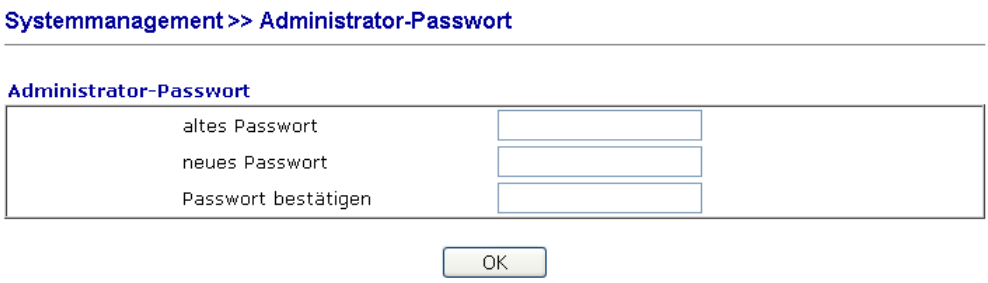
CPE-Client - Hier braucht nichts eingegeben zu werden. Die Information ist für den ACS nützlich.

Aktiv/Inaktiv – Manchmal können Port-Konflikte auftreten. Um solche Probleme zu lösen, können Sie die Port-Nummer für CPE ändern. Klicken Sie auf Aktiv und ändern Sie die Port-Nummer.

Periodische Informationsübertragung zum ACS-Server - Die Standardeinstellung ist **Aktiv**. Geben Sie die Intervalle oder Zeiten an, zu denen der Router das CPE benachrichtigen soll. Um die Benachrichtigung zu deaktivieren, klicken Sie auf Inaktiv.

5.14.3 Administratorpasswort

Auf dieser Seite können Sie ein neues Passwort setzen:



Altes Passwort - Geben Sie das alte Passwort ein. Per Werkseinstellung ist das Passwort leer.

Neues Passwort - Geben Sie das neue Passwort in diesem Feld ein.

Passwort bestätigen - Geben Sie das neue Passwort erneut ein.

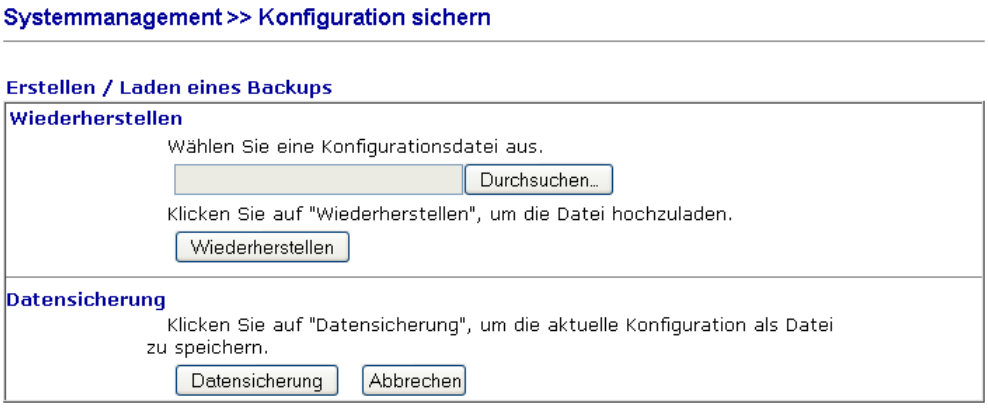
Wenn Sie auf OK klicken, erscheint das Anmeldefenster. Bitte benutzen Sie das neue Passwort, um sich erneut im Router-Menü anzumelden.

5.14.4 Sicherung der Konfiguration

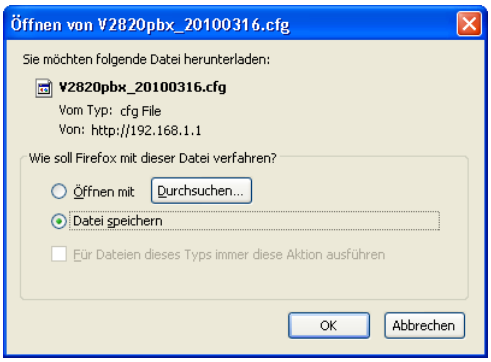
Konfiguration sichern

Befolgen Sie die folgenden Schritte, um Ihre Konfiguration zu sichern.

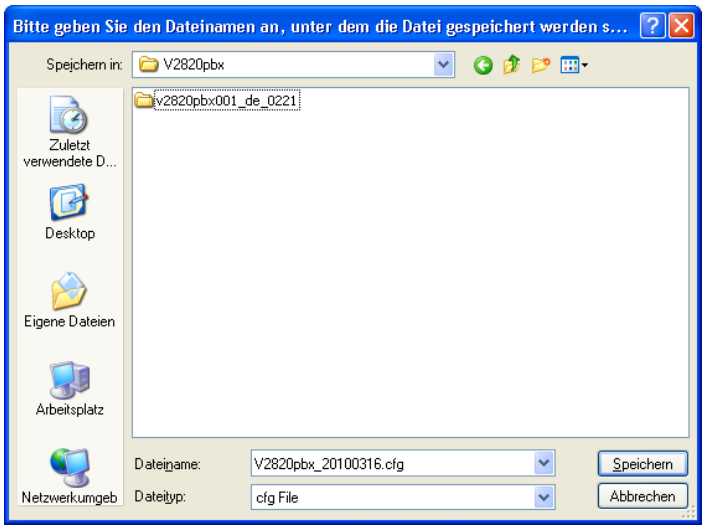
1. Gehen Sie zu **Systemmanagement** >> **Konfiguration sichern**. Das folgende Fenster erscheint wie unten abgebildet.



2. Klicken Sie auf **Datensicherung**, um in den folgenden Dialog zu gelangen. Klicken Sie dann auf **Speichern**, um einen weiteren Dialog zu öffnen, in dem Sie die Konfiguration in eine Datei speichern können.



3. Der Standard-Dateiname im Dialog **Speichern unter** ist **config.cfg**. Sie können jedoch auch einen anderen Namen zuweisen.



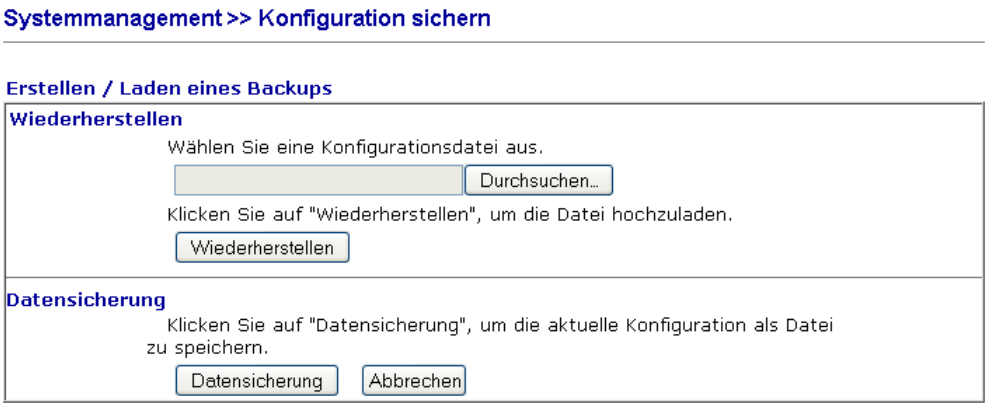
4. Klicken Sie auf **Speichern**, um die Konfiguration automatisch in eine Datei namens **config.cfg** auf Ihren Rechner herunterzuladen.

Das obige Beispiel verwendet die **Windows**-Plattform. Die **Mac**- oder **Linux**-Plattformen zeigen zwar unterschiedliche Dialoge an, die Sicherungsfunktion ist jedoch trotzdem verfügbar.

Hinweis: Die Zertifikate müssen gesondert gesichert werden. Das Konfigurations-Backup schließt die Zertifikatinformationen nicht ein.

Konfiguration wiederherstellen

1. Gehen Sie zu **Systemmanagement** >> **Konfiguration sichern**. Das folgende Fenster erscheint wie unten abgebildet.

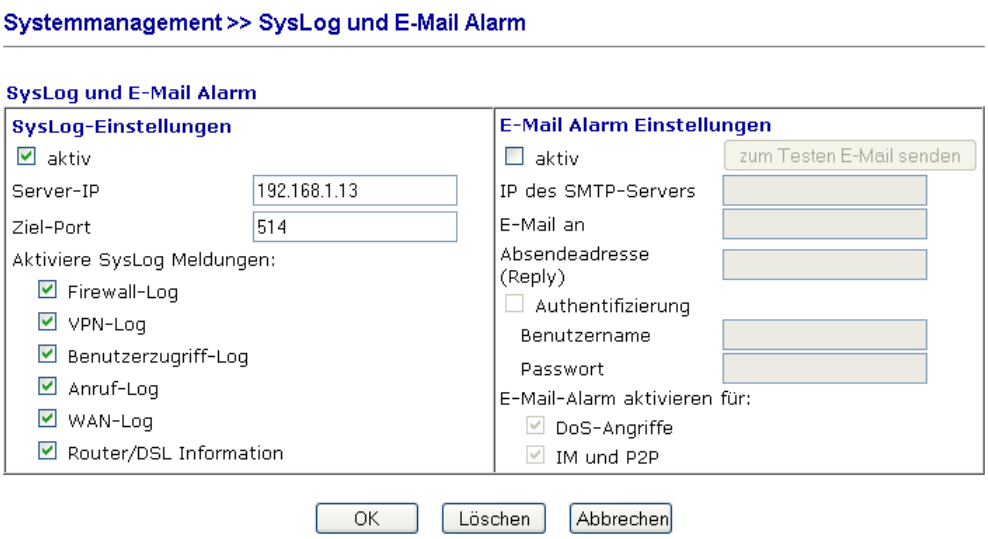


2. Klicken Sie auf **Durchsuchen**, um die für den Router zu ladende Konfigurationsdatei auszuwählen.

3. Klicken Sie auf **Wiederherstellen** und warten Sie ein paar Sekunden, bis das folgende Bild erscheint und bestätigt, dass der Wiederherstellungsprozess erfolgreich war.

5.14.5 Syslog/Mail-Alarm

Die Syslog-Funktion dient der Überwachung des Routers durch den Benutzer. Dank dieser Funktion ist es nicht nötig, sich für die Fehlersuche im Konfigurationsmenü anzumelden.



Aktiv (Syslog…) - Markieren Sie **Aktiv**, um die Syslog-Funktion zu aktivieren.

Syslog Server-IP - IP-Adresse des Syslog-Servers.

Ziel-Port - Bestimmen Sie einen Port für das Syslog-Protokoll.

Aktiviere SysLog Meldungen - Markieren Sie das Kästchen in diesem Dialog, um die entsprechenden Meldungen über Firewall, VPN, Benutzerzugriff, Anrufe, WAN und Router/DSL an Syslog zu senden.

Aktiv (Alarmeinstellungen…) - Markieren Sie **Aktiv**, um die Mail-Alarmfunktion zu aktivieren.

Test-E-Mail versenden - Testet die auf dieser Seite angegebene E-Mail-Adresse. Bitte geben Sie zuerst die E-Mail-Adresse an und klicken dann auf diese Taste, um zu überprüfen, ob die E-Mail-Adresse erreichbar ist oder nicht.

SMTP-Server - IP-Adresse des SMTP-Servers.

E-Mail an - Geben Sie eine Mail-Adresse für ausgehende Mails an.

Absendeadresse (Reply) - Geben Sie die E-Mail-Adresse einer anderen Mailbox an, an welche alle von der Empfängeradresse abgelehnten Mails zugestellt werden können.

Die hier eingegebene E-Mail-Adresse dient auch als Absenderadresse, wenn Vigor Warnmeldungen versendet.

Authentifizierung - Markieren Sie dieses Kästchen, um diese Funktion während der Nutzung der E-Mail-Anwendung zu aktivieren.

Benutzername - Geben Sie den Benutzernamen für die Authentisierung ein.

Passwort - Geben Sie das Authentisierungspasswort ein.

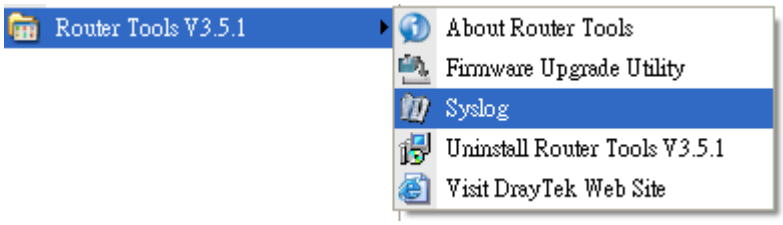
E-Mail-Alarm aktivieren für - Markieren Sie das Kästchen, damit Warnmeldungen an das E-Mail-Postfach gesendet werden, wenn das Modem die hier angegebenen Umstände erkennt.

Klicken Sie auf **OK**, um diese Einstellungen zu speichern.

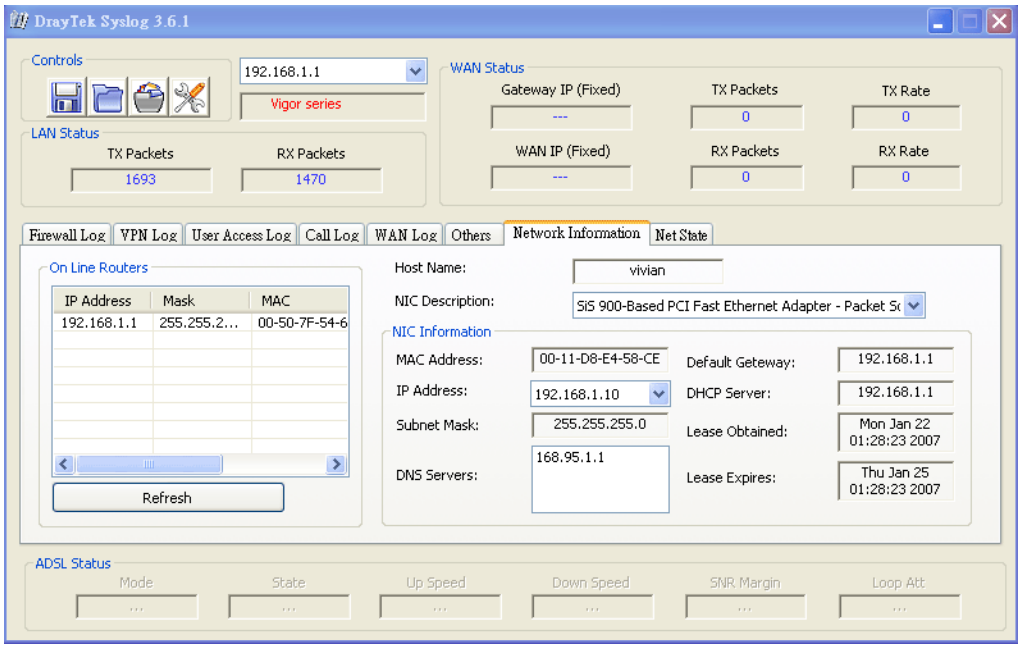
Gehen Sie wie folgt vor, um das Syslog zu betrachten:

1. Geben Sie die IP-Adresse des beobachtenden Rechners im Feld für die Server-IP-Adresse ein.

2. Installieren Sie die Router Tools im **Utility**-Menü auf der mitgelieferten CD. Wählen Sie nach der Installation aus dem Programmmenü **Router Tools>>Syslog**.



3. Wählen Sie im Syslog-Menü den Router, den Sie überwachen möchten. Dazu müssen Sie unter **Network Information** die Netzwerkkarte wählen, über die der Rechner mit dem Router verbunden ist. Ansonsten können Sie keine Informationen vom Router erhalten.



5.14.6 Zeit und Datum

Hier können Sie angeben, wo der Router die Uhrzeit abfragen soll.

Aktuelle Systemzeit - Klicken Sie auf **Zeit abrufen**, um die aktuelle Zeit zu erhalten.

Rechner-/Browserzeit - Wählen Sie diese Option, um die Browser-Zeit des entfernten Rechners des Administrators als Systemzeit

für den Router zu verwenden.

Internet-Zeit - Wählen Sie diese Option, um die Zeit über das gewählte Protokoll von Zeitservern im Internet abzufragen.

Zeitprotokoll - Auswahl des Zeitprotokolls.

Server-IP - IP-Adresse des Zeitservers eingeben.

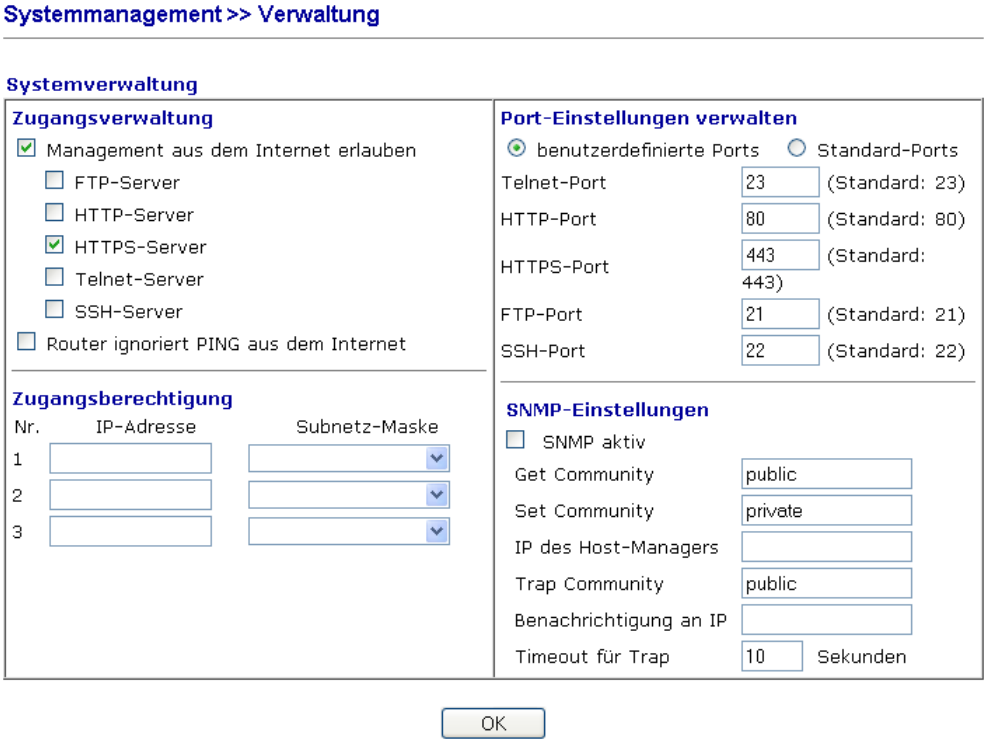
Zeitzone - Zeitzone auswählen, in der sich der Router befindet.

Aktualisierungsintervall - Wählen Sie ein Zeitintervall für die Aktualisierung vom NTP-Server.

Klicken Sie auf **OK**, um diese Einstellungen zu speichern.

5.14.7 Verwaltung

Auf dieser Seite können Sie die Einstellungen zur Zugriffskontrolle, Zugriffsliste, Port-Konfiguration und SNMP-Konfiguration verwalten. Zur Verwaltung der Zugriffskontrolle wird beispielsweise die Portnummer verwendet, um die SIP-Meldung zum Aufbau einer Sitzung zu senden/empfangen. Für VoIP-Anrufe muss der Standardwert von 5060 dem Wert des entfernten Registrars entsprechen.



Management aus dem Internet erlauben - Aktivieren Sie dieses Kästchen, um Systemadministratoren zu ermöglichen, sich aus dem Internet anzumelden. Das System bietet verschiedene Server, um den Router aus dem Internet zu verwalten. Haken Sie das/die entsprechenden Kästchen an.

Router ignoriert PING aus dem Internet -

Aktivieren Sie dieses Kästchen, um alle Ping-Pakete aus dem Internet zu verwerfen. Diese Funktion ist aus Sicherheitsgründen standardmäßig aktiviert.

Zugangsberechtigung - Sie können bestimmen, dass sich der Systemadministrator nur von einem in der Liste angegebenen Host oder Netzwerk anmelden kann. Es können bis zu drei IPs/Subnetz-Masken angegeben werden.

Nr. IP - Zeigt eine IP-Adresse an, der gestattet wird, sich am Router anzumelden.

Subnetz-Maske - Zeigt eine Subnetz-Maske an, der gestattet wird, sich am Router anzumelden.

Standard-Ports - Markieren, um die Standard-Port-Nummern für die Telnet- und HTTP-Server zu verwenden.

Benutzerdefinierte Ports - Markieren, um benutzerdefinierte Portnummern für die Telnet-, HTTP- und FTP-Server anzugeben.

SNMP aktiv - Markieren, um diese Funktion zu aktivieren.

Get Community - Geben Sie einen Namen für die Get Community ein. Die Standardeinstellung ist **public.**

Set Community - Geben Sie einen Namen für die Community ein. Die Standardeinstellung ist **private.**

IP des Host-Managers - Bestimmen Sie einen Host als Manager, um die SNMP-Funktion auszuführen. Geben Sie die IP-Adresse des Hosts ein.

Trap Community - Geben Sie einen Namen für die Trap Community ein. Die Standardeinstellung ist **public.**

Benachrichtigung an IP - Geben Sie die IP-Adresse des Hosts an, der die Trap Community erhalten soll.

Timeout für Trap - Die Standardeinstellung ist 10 Sekunden.

5.14.8 Neustart

Der Router kann aus dem Konfigurationsmenü heraus neu gestartet werden. Wählen Sie **Neustart** unter **Systemmanagement**, um die folgende Seite zu öffnen:

Falls Sie den Router mit der aktuellen Konfiguration neu starten möchten, wählen Sie **Aktuelle Konfiguration verwenden** und klicken auf **OK**. Um den Router auf die Werkseinstellungen zurückzusetzen, wählen Sie **Auf Werkseinstellung zurücksetzen** und klicken auf **OK**. Der Router benötigt fünf Sekunden, um das System neu zu starten.

Hinweis: Wenn das System nach Konfiguration der Internet-Einstellungen die Web-Seite für den Neustart des Systems anzeigt, klicken Sie bitte auf **OK**, um Ihren Router neu zu starten und so den ordnungsgemäßen Betrieb sicherzustellen und unerwartete Router-Probleme in der Zukunft zu vermeiden.

5.14.9 Firmware aktualisieren

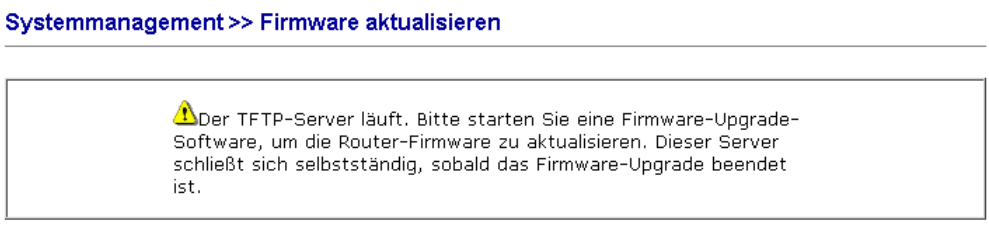
Um Ihre Router-Firmware zu aktualisieren müssen Sie das **Firmware Upgrade Utility** installieren, welches Sie von der beigefügten CD oder über unsere Homepage www.draytek.de erhalten. Der folgende Dialog erläutert die Aktualisierung der Firmware anhand eines Beispiels. Das Beispiel verwendet das Windows-Betriebssystem.

Laden Sie die neueste Firmware von der DrayTek-Web-Site oder -FTP-Site herunter. Die Draytek-Web-Site ist www.draytek.de, die FTP-Site ist ftp.draytek.com.

Wählen Sie **Systemmanagement>> Firmware aktualisieren**, um das Firmware Upgrade Utility zu starten.

Systemmanagement >> Firmware aktualisieren
Online Firmware-Upgrade
Wählen Sie eine Firmware Datei.
Durchsuchen...
Klicken Sie Upgrade, um die Firmware hochzuladen.
Upgrade
TFTP Firmware-Upgrade von LAN
aktuelle Firmwareversion: 3.5.4_2111112
Firmware-Upgrade Prozedur:
1. Unten durch Bestätigen des "OK"-Buttons den TFTP-Server starten.
2. Starten von DrayTek's Firmware-Upgrade-Utility oder einer anderen TFTP-Software.
3. Firmwaredatei auswählen.
4. Datei an Router senden.
5. Der TFTP-Server wird nach dem Download automatisch beendet.
Möchten Sie die Firmware aktualisieren?
OK

Klicken Sie auf **OK**. Der folgende Dialog erscheint. Bitte führen Sie zunächst die Firmware-Aktualisierung durch.


Systemmanagement >> Firmware aktualisieren
Der TFTP-Server läuft. Bitte starten Sie eine Firmware-Upgrade-Software, um die Router-Firmware zu aktualisieren. Dieser Server schließt sich selbstständig, sobald das Firmware-Upgrade beendet ist.

Einzelheiten zur Aktualisierung der Firmware werden in Kapitel 4 erläutert.

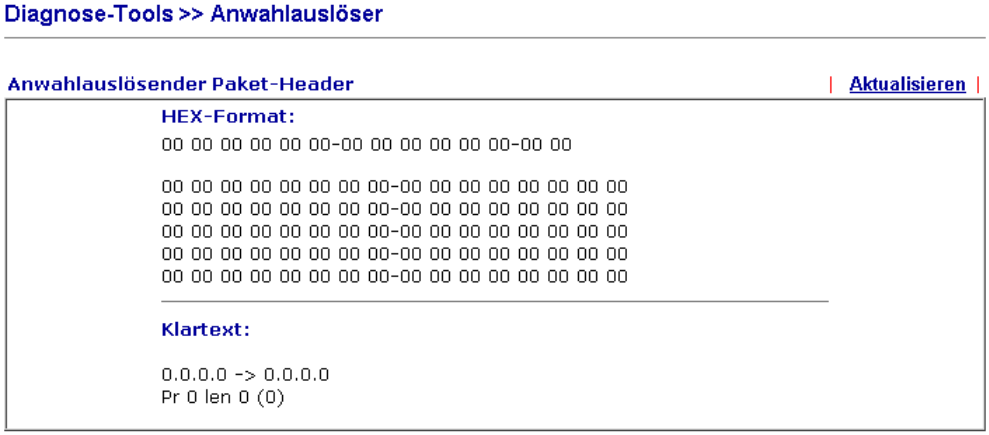
5.15 Diagnose-Tools

Die Diagnose-Tools eignen sich zur **Kontrolle** oder **Diagnose** des Status Ihres Vigor-Routers.

Die folgende Abbildung zeigt die Menüeinträge für die Diagnose-Tools:

5.15.1 Anwahlauslöser

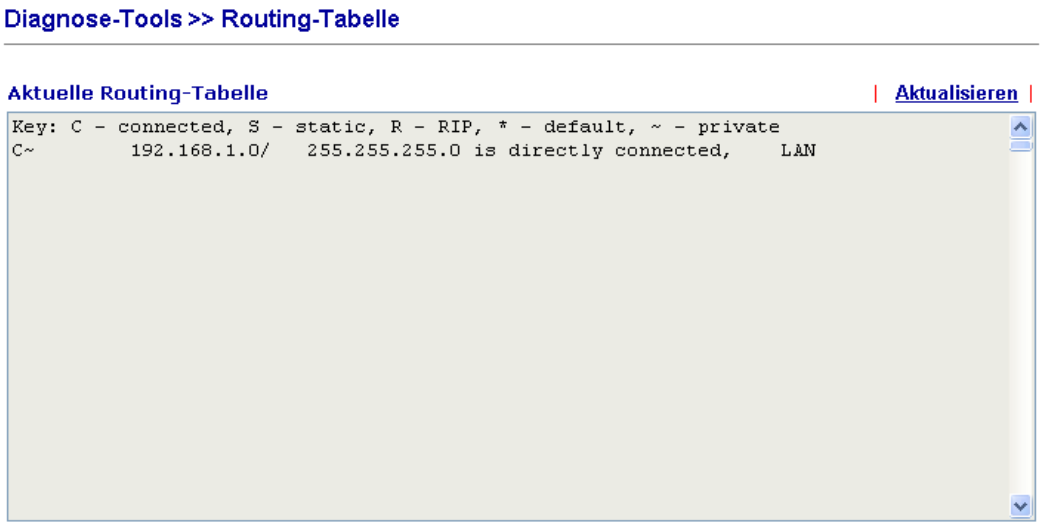
Wählen Sie **Diagnose-Tools** und klicken auf **Anwahlauslöser**, um den Dialog zu öffnen. Die Internet-Verbindung (z.B. ISDN, PPPoE, PPPoA usw.) wird von einem Paket von der Quell-IP-Adresse angestoßen.



Klartext	Zeigt die Quell-IP-Adresse (lokal), die Ziel-IP-Adresse (entfernt), das Protokoll und die Länge des Pakets an.
Aktualisieren	Anklicken, um die Seite neu zu laden.

5.15.2 Routing-Tabelle

Wählen Sie **Diagnose-Tools** und klicken auf **Routing-Tabelle**, um den Dialog zu öffnen.


Diagnose-Tools >> Routing-Tabelle
Aktuelle Routing-Tabelle
| Aktualisieren |
Key: C - connected, S - static, R - RIP, * - default, ~ - private
C~ 192.168.1.0/ 255.255.255.0 is directly connected, LAN

Aktualisieren	Anklicken, um die Seite neu zu laden.

5.15.3 ARP-Cache-Tabelle

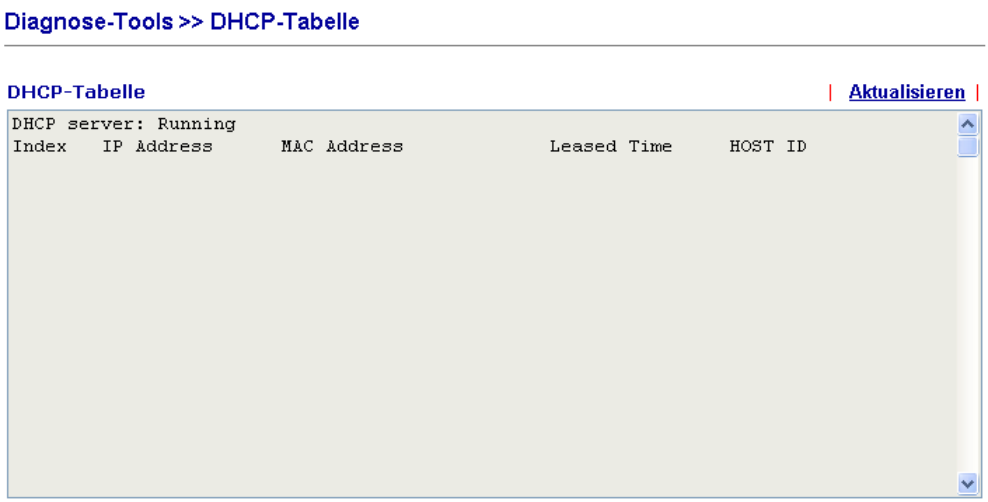
Klicken Sie auf **Diagnose-Tools** und wählen Sie **ARP-Cache-Tabelle**, um den Inhalt des ARP-Caches (Address Resolution Protocol) im Router zu betrachten. Die Tabelle zeigt die Zuordnung zwischen den Ethernet-Hardware-Adressen (MAC-Adressen) und IP-Adressen an.

Aktualisieren	Anklicken, um die Seite neu zu laden.
Löschen	Anklicken, um die gesamte Tabelle zu löschen.

5.15.4 DHCP-Tabelle

Diese Tabelle liefert Informationen zur Zuweisung von IP-Adressen. Diese Informationen sind nützlich für die Diagnose von Netzwerkproblemen wie IP-Adressenkonflikte usw.

Wählen Sie **Diagnose-Tools** und klicken auf **DHCP-Tabelle**, um den Dialog zu öffnen.



Index - Zeigt die Verbindungsnummer an.

IP-Adresse - Zeigt die IP-Adresse an, die dieser Router dem angegebenen Rechner zugewiesen hat.

MAC-Adresse - Zeigt die MAC-Adresse des angegebenen Rechners an, dem per DHCP eine IP-Adresse zugewiesen wurde.

Lease Time - Zeigt die Lease Time des angegebenen Rechners an.

Host ID - Zeigt die Host-ID des angegebenen Rechners an.

Aktualisieren - Anklicken, um die Seite neu zu laden.

5.15.5 NAT-Sitzungstabelle

Wählen Sie **Diagnose-Tools** und klicken auf **NAT-Tabelle**, um auf die Konfigurationsseite zu gelangen.

Diagnose-Tools >> NAT-Tabelle
NAT-Tabelle aktiver Sitzungen
| Aktualisieren |
Private IP :Port #Pseudo Port Peer IP :Port Interface

Private IP:Port - Gibt die Quell-IP-Adresse und den Port des lokalen Rechners an.

#Pseudo-Port - Gibt den zeitweiligen Port des Routers an, der für NAT verwendet wird.

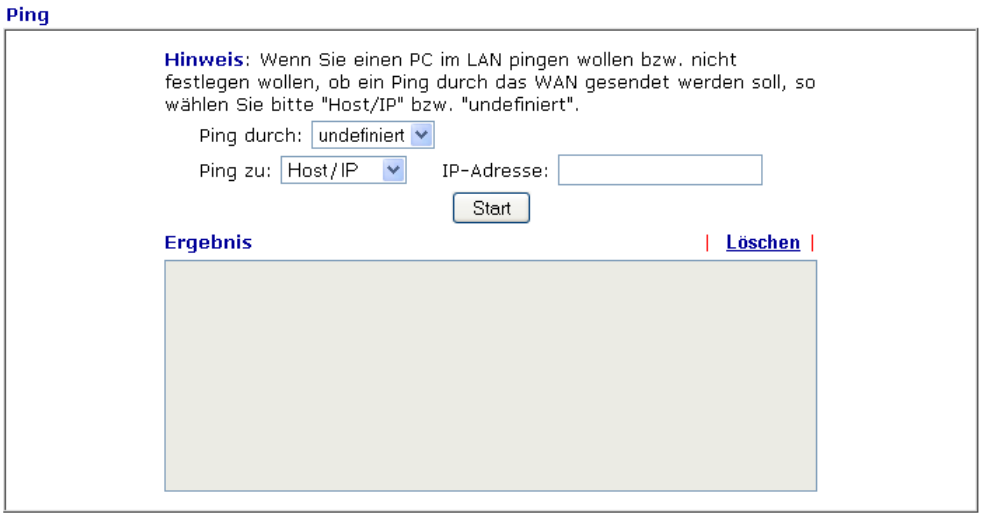
Peer-IP:Port - Zeigt die Ziel-IP-Adresse und den Port des entfernten Hosts an.

Schnittstelle - Zeigt die entsprechende Nummer der Schnittstelle an.

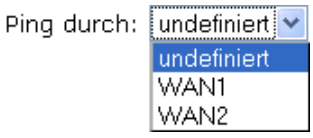
Aktualisieren - Anklicken, um die Seite neu zu laden.

5.15.6 Ping

Wählen Sie **Diagnose-Tools** und klicken auf **Ping**, um den Dialog zu öffnen.


Diagnose-Tools >> Ping
Ping
Hinweis: Wenn Sie einen PC im LAN pingen wollen bzw. nicht festlegen wollen, ob ein Ping durch das WAN gesendet werden soll, so wählen Sie bitte "Host/IP" bzw. "undefiniert".
Ping durch: undefiniert
Ping zu: Host/IP
IP-Adresse:
Start
Ergebnis
| Löschen |

Ping durch - Verwenden Sie die Dropdown-Liste, um die WAN-Schnittstelle zu wählen, durch die Sie pingen möchten, oder wählen Sie **Undefiniert**, um diese vom Router automatisch bestimmen zu lassen.



Ping zu - Verwenden Sie die Dropdown-Liste, um das Ziel zu wählen, das Sie anpingen möchten.

IP-Adresse - Geben Sie die IP-Adresse des Hosts ein, den Sie anpingen möchten.

Start - Klicken Sie auf diese Schaltfläche, um Ping zu starten. Das Ergebnis wird auf dem Bildschirm angezeigt.

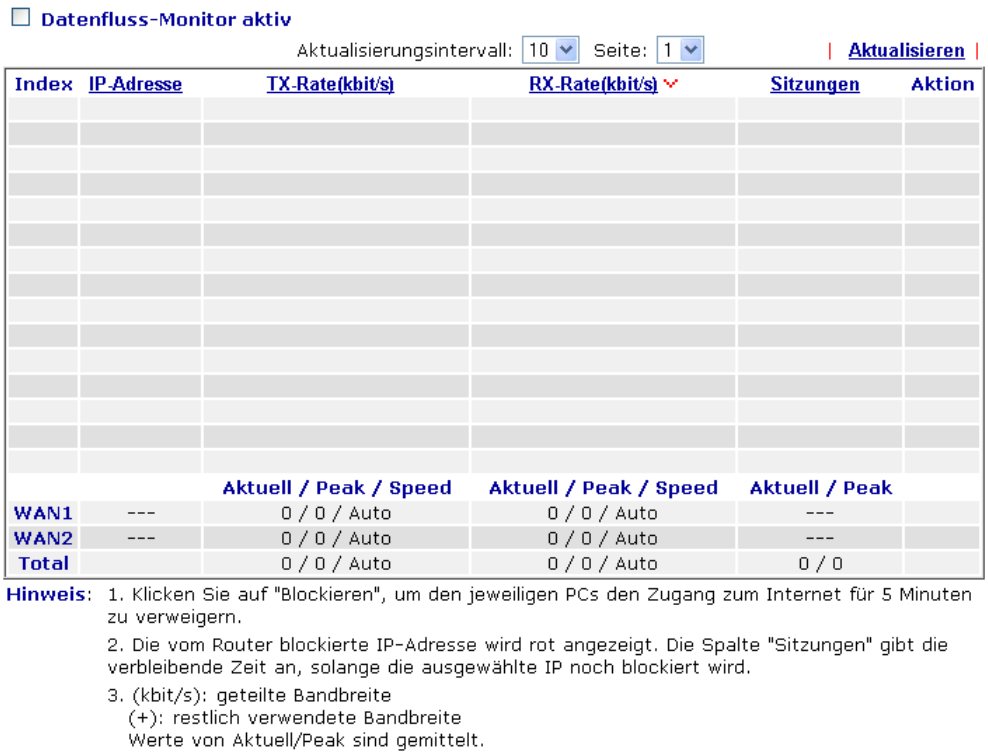
Löschen - Klicken Sie auf diesen Link, um die Ausgabe im Fenster zu löschen.

5.15.7 Datenfluss-Monitor

Diese Seite zeigt die Aktivität der überwachten IP-Adresse an und aktualisiert die Daten alle paar Sekunden. Die hier angezeigte IP-Adresse wird im Bandbreitenmanagement konfiguriert. Sie müssen IP-Bandbreitenbegrenzung und IP-Sitzungsbegrenzung aktivieren, bevor Sie den Datenfluss-Monitor starten. Falls dies nicht bereits geschehen ist, erscheint eine Meldung, die Sie daran erinnert.

Wählen Sie **Diagnose-Tools** und klicken auf **Datenfluss-Monitor**, um den Dialog zu öffnen. Klicken Sie auf **IP-Adresse**, **TX-Rate**, **RX-Rate** oder **Sitzungen**, um sich die entsprechenden Daten anzeigen zu lassen.

Diagnose-Tools >> Datenfluss-Monitor


Datenfluss-Monitor aktiv
Aktualisierungsintervall: 10 Seite: 1
Aktualisieren
Index
IP-Adresse
TX-Rate(kbit/s)
RX-Rate(kbit/s)
Sitzungen
Aktion
Aktuell / Peak / Speed
Aktuell / Peak / Speed
Aktuell / Peak
WAN1 --- 0 / 0 / Auto 0 / 0 / Auto ---
WAN2 --- 0 / 0 / Auto 0 / 0 / Auto ---
Total 0 / 0 / Auto 0 / 0 / Auto 0 / 0
Hinweis: 1. Klicken Sie auf "Blockieren", um den jeweiligen PCs den Zugang zum Internet für 5 Minuten zu verweigern.
2. Die vom Router blockierte IP-Adresse wird rot angezeigt. Die Spalte "Sitzungen" gibt die verbleibende Zeit an, solange die ausgewählte IP noch blockiert wird.
3. (kbit/s): geteilte Bandbreite
(+): restlich verwendete Bandbreite
Werte von Aktuell/Peak sind gemittelt.

Datenfluss-Monitor aktiv Markieren Sie dieses Kästchen, um diese Funktion zu aktivieren.

AktualisierungsintervallVerwenden Sie die Dropdown-Liste, um das automatische Aktualisierungsintervall (in Sekunden) des Datenfluss-Monitors zu bestimmen.

AktualisierenKlicken Sie auf diesen Link, um diese Seite manuell zu aktualisieren.

IndexNummer des Datenflusses anzeigen.

IP-AdresseIP-Adresse des überwachten Geräts anzeigen.

Übertragungsgeschwindigkeit (kbit/s)Übertragungsgeschwindigkeit des überwachten Geräts anzeigen.

Empfangsgeschwindigkeit (kbit/s) Empfangsgeschwindigkeit des überwachten Geräts anzeigen.

SitzungenZeigt die Anzahl der Sitzungen an, die Sie unter Sitzungen begrenzen angegeben haben.

AktionBlockieren - Sperrt den Internetzugang für den angegebenen PC für fünf Minuten.

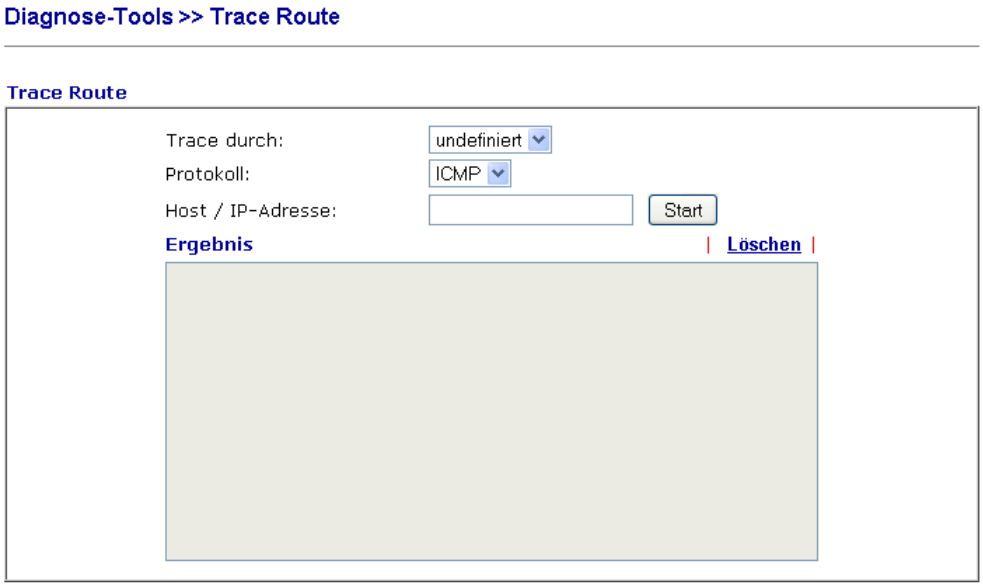
Freigeben – Das Gerät mit der entsprechenden IP-Adresse wird freigegeben.

5.15.8 Traffic-Diagramm

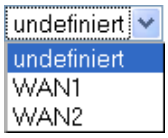
Wählen Sie **Diagnose-Tools** und klicken auf **Traffic-Diagramm**, um den Dialog zu öffnen. Sie können WAN1 Bandbreite/WAN2 Bandbreite, Sitzungen, täglich oder wöchentlich wählen, um verschiedene Traffic-Diagramme zu betrachten. Sie können jederzeit auf **Aktualisieren** klicken, um das Diagramm zu aktualisieren.

5.15.9 Trace Route

Wählen Sie **Diagnose-Tools** und klicken auf **Trace Route**, um den Dialog zu öffnen. Auf dieser Seite können Sie den Pfad vom Router zum Host nachverfolgen. Geben Sie einfach die IP-Adresse des Hosts im Feld ein und klicken auf **Ausführen**. Das Ergebnis wird auf dem Bildschirm angezeigt.



Trace durch - Verwenden Sie die Dropdown-Liste, um die WAN-Schnittstelle zu wählen, durch die Sie pingen möchten, oder wählen Sie **Undefiniert**, um diese vom Router automatisch bestimmen zu lassen.



Protokoll - Wählen Sie für die Route ein Protokoll (ICMP oder UDP).

Host/IP-Adresse - Zeigt die Host-IP-Adresse an.

Start - Klicken Sie auf diese Taste, um Trace Route zu starten.

Löschen - Klicken Sie auf diesen Link, um die Ausgabe im Fenster zu löschen.

Kapitel 6: Fehlersuche

Dieser Abschnitt hilft Ihnen, Probleme zu lösen, falls Sie nach Installation des Routers und Abschluss der Web-Konfiguration keinen Zugang zum Internet haben. Bitte folgen Sie den Anweisungen, um Ihre Basiskonfiguration schrittweise zu überprüfen.

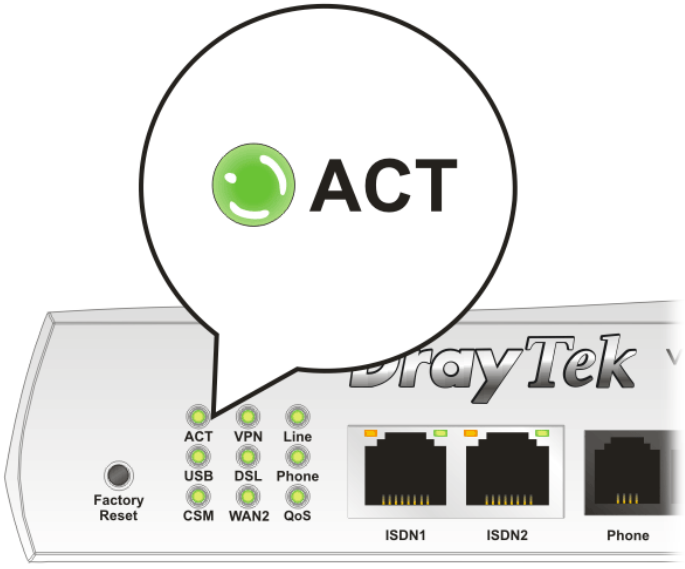
- Hardwarestatus überprüfen.
- Kontrollieren, ob die Netzwerkverbindungseinstellungen auf Ihrem Rechner in Ordnung sind.
- Pingen des Routers von Ihrem PC aus.
- Prüfen der ISP-Einstellungen.
- Falls erforderlich, auf Werkseinstellungen zurücksetzen.

Falls der Router immer noch nicht ordnungsgemäß funktioniert, obwohl Sie alle beschriebenen Schritte durchgeführt haben, ist es an der Zeit, sich für weitere Unterstützung an Ihren Händler zu wenden.

6.1 Hardwarestatus überprüfen

Befolgen Sie die folgenden Schritte, um den Hardware-Status zu kontrollieren:

1. Überprüfen Sie die Stromversorgung und die LAN-Kabelverbindungen. Sehen Sie zu Einzelheiten Abschnitt **1.3** "**Hardwareinstallation**".
2. Schalten Sie den Router ein. Die **ACT LED** muss einmal pro Sekunde blinken, und die **LAN LED** muss leuchten.



3. Falls dies nicht der Fall ist, ist der Hardwarestatus nicht in Ordnung. Gehen Sie zurück zu **1.3** "**Hardwareinstallation**", um die Hardwareinstallation nochmals auszuführen. Danach versuchen Sie es erneut.

6.2 Netzwerkeinstellungen am PC kontrollieren

Manchmal funktionieren Links aufgrund falscher Netzwerkverbindungseinstellungen nicht. Falls ein Link trotz Anwendung der Anweisungen im obigen Abschnitt immer noch nicht funktioniert, folgen Sie bitten den folgenden Anweisungen, um zu kontrollieren, ob die Netzwerkverbindungseinstellungen in Ordnung sind.

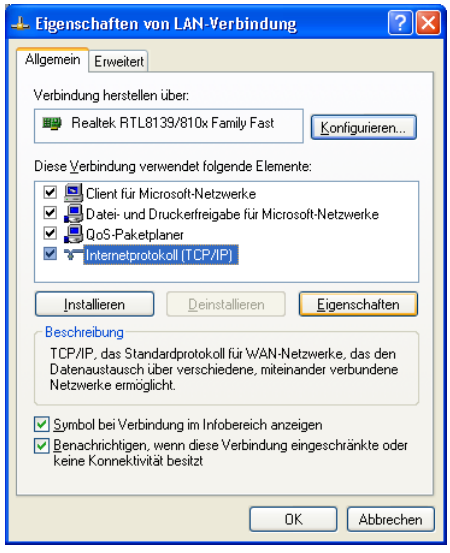
Für Windows

> Das Beispiel verwendet Windows XP. Sofern die Schritte für andere Betriebssysteme nicht ähnlich sind, sehen Sie bitte die Hinweise unter **www.draytek.de**.

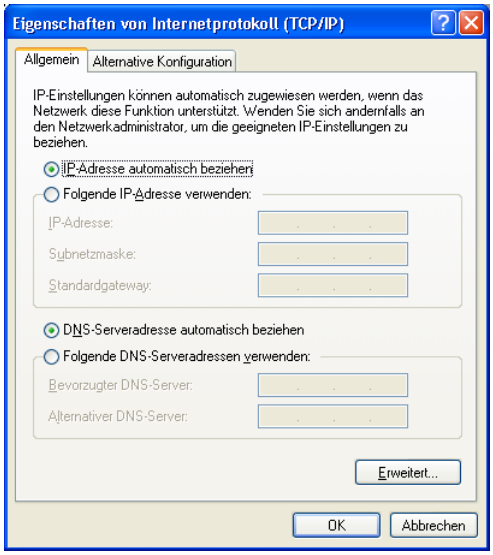
1. Gehen Sie zur **Systemsteuerung → Netzwerkverbindungen**

2. Klicken Sie die **LAN-Verbindung** mit der rechten Maustaste an und klicken Sie auf **Eigenschaften**.

3. Wählen Sie das **Internetprotokoll (TCP/IP)** und klicken Sie auf **Eigenschaften**.

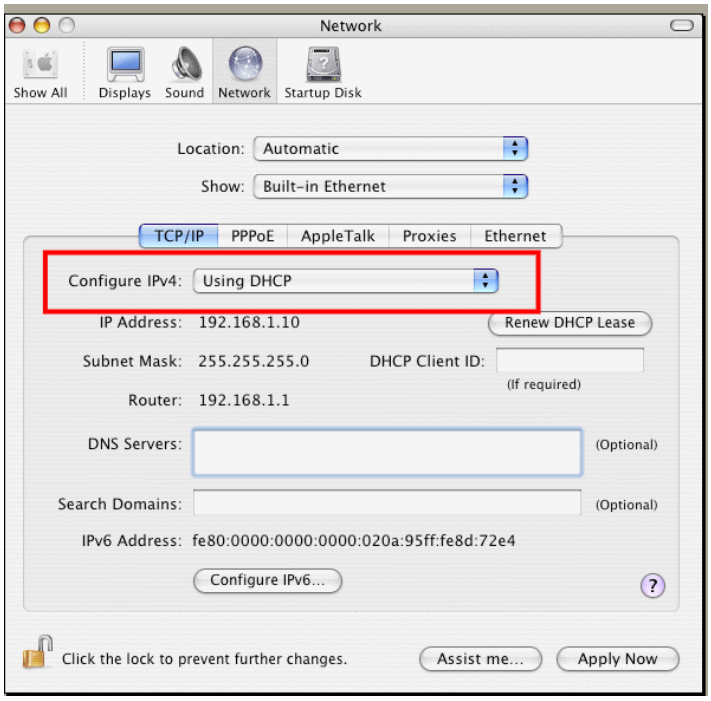


4. Wählen Sie **IP-Adresse automatisch beziehen** und **DNS-Serveradresse automatisch beziehen**.



Für MacOS

1. Klicken Sie in MacOS doppelt auf den Arbeitsbereich.
2. Öffnen Sie den Ordner **Programme** und wählen Sie **Netzwerk**.
3. Im Menü **Netzwerk** wählen Sie **DHCP** aus der Dropdown-Liste **IPv4 konfigurieren**.



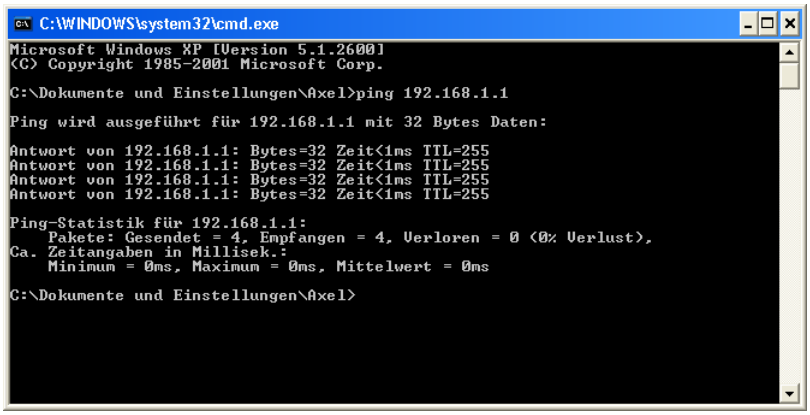
6.3 Pingen des Routers von Ihrem PC aus

Die Standard-Gateway-IP-Adresse des Routers ist 192.168.1.1. Es mag notwendig sein, den Befehl "ping" zu verwenden, um den Verbindungsstatus des Routers zu kontrollieren. **Es ist wichtig, dass der Rechner eine Antwort von 192.168.1.1 erhält.** Falls dies nicht geschieht, überprüfen Sie bitte die IP-Adresse Ihres Rechners. Wir empfehlen, die Netzwerkverbindung so zu konfigurieren, dass die IP automatisch bezogen wird (siehe Abschnitt 6.2).

Befolgen Sie die folgenden Schritte, um den Router anzupingen.

Für Windows

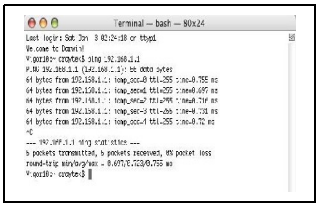
1. Öffnen Sie die **Eingabeaufforderung** (unter **Start> Ausführen**).
2. Geben Sie **command** (Windows 95/98/ME) bzw. **cmd** (Windows NT/2000/XP/Vista) ein. Die DOS-Eingabeaufforderung erscheint.


C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Dokumente und Einstellungen\Axel>ping 192.168.1.1
Ping wird ausgeführt für 192.168.1.1 mit 32 Bytes Daten:
Antwort von 192.168.1.1: Bytes=32 Zeit<1ms TTL=255
Antwort von 192.168.1.1: Bytes=32 Zeit<1ms TTL=255
Antwort von 192.168.1.1: Bytes=32 Zeit<1ms TTL=255
Antwort von 192.168.1.1: Bytes=32 Zeit<1ms TTL=255
Ping-Statistik für 192.168.1.1:
Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0 (0% Verlust),
Ca. Zeitangaben in Millisek.:
Minimum = 0ms, Maximum = 0ms, Mittelwert = 0ms
C:\Dokumente und Einstellungen\Axel>

3. Geben Sie ping 192.168.1.1 ein und drücken auf [Enter]. Falls der Link in Ordnung ist, erscheint die Zeile "**Reply from 192.168.1.1:bytes=32 time<1ms TTL=255**".
4. Falls diese Zeile nicht erscheint, kontrollieren Sie bitte die IP-Adresse Ihres Rechners.

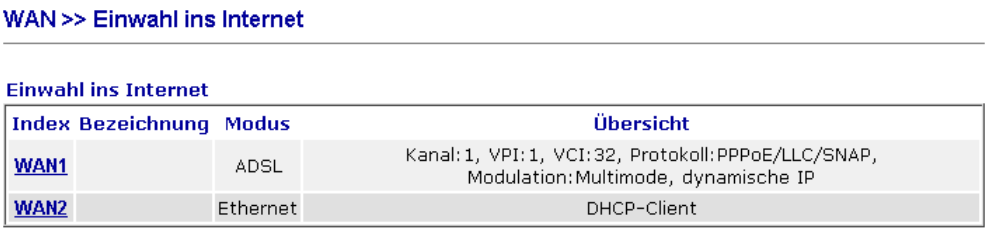
Für MacOS (Terminal)

1. Klicken Sie in MacOS doppelt auf den Arbeitsbereich.
2. Öffnen Sie den Ordner **Programme** und wählen Sie **Dienstprogramme**.
3. Klicken Sie **Terminal** doppelt an. Das Terminalfenster erscheint.
4. Geben Sie **ping 192.168.1.1** ein und drücken auf [Enter]. Falls der Link in Ordnung ist, erscheint die Zeile "**64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=xxxx ms**".



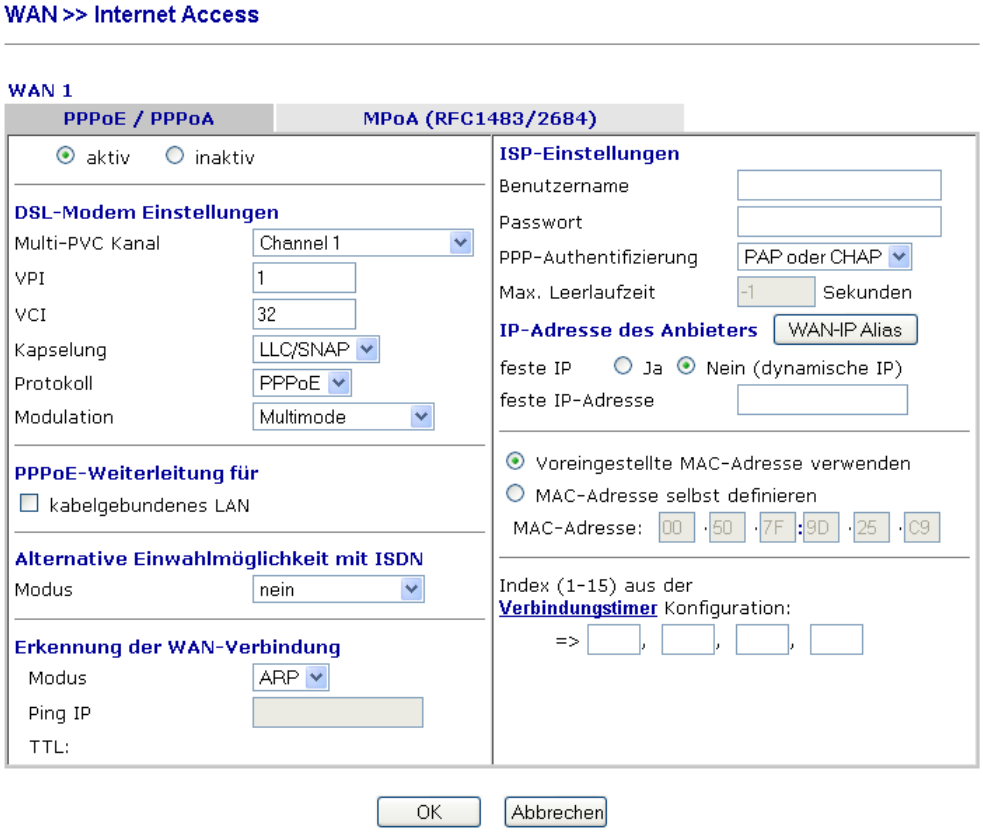
6.4 Prüfen der ISP-Einstellungen

Klicken Sie auf **WAN>> Einwahl ins Internet** und kontrollieren Sie, ob die ISP-Einstellungen korrekt sind. Klicken Sie auf WAN1 oder WAN2, um die zuvor konfigurierten Einstellungen zu überprüfen.


WAN >> Einwahl ins Internet
Einwahl ins Internet
Index Bezeichnung Modus Übersicht
WAN1 ADSL Kanal: 1, VPI: 1, VCI: 32, Protokoll: PPPoE/LLC/SNAP, Modulation: Multimode, dynamische IP
WAN2 Ethernet DHCP-Client

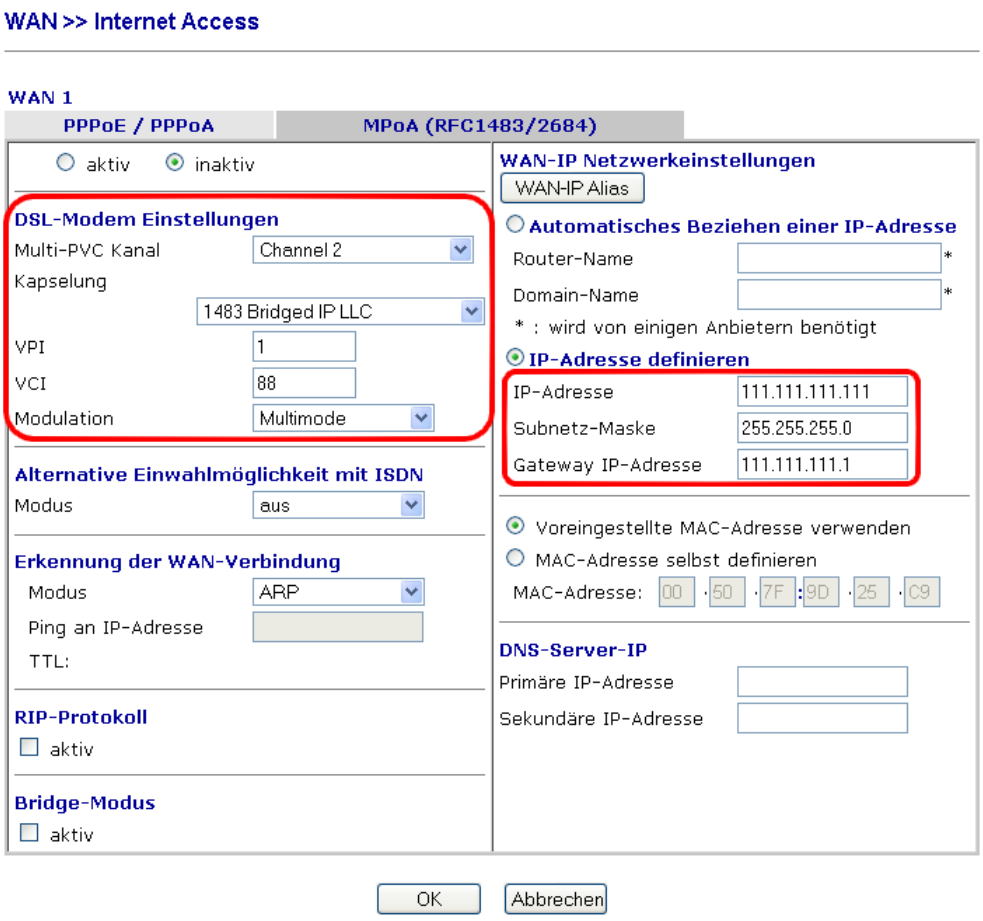
Für PPPoE-Benutzer

1. Prüfen Sie, ob **Aktiv** gewählt ist.
2. Prüfen Sie, ob der **Benutzername** und das **Passwort** den von Ihrem **ISP** erhaltenen Werten entsprechen.



Für MPoA-Benutzer

1. Prüfen Sie, ob **Aktiv** gewählt ist.

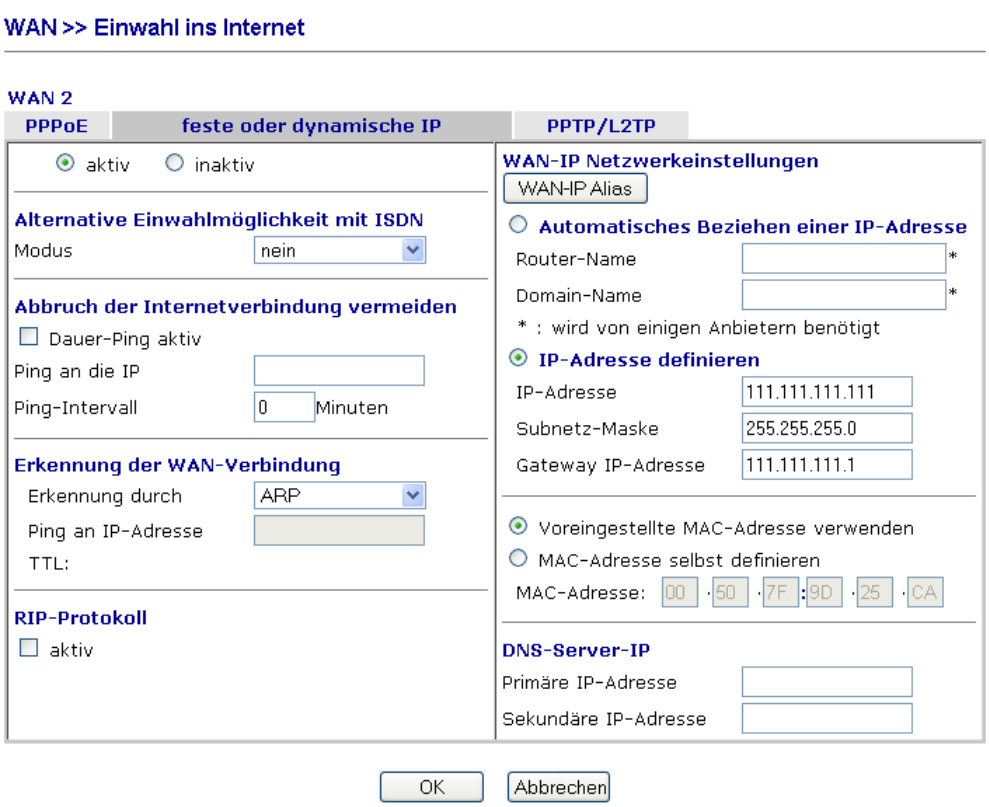


2. Prüfen Sie, ob die **DSL-Modemeinstellungen** korrekt sind.

Prüfen Sie, ob **IP-Adresse, Subnetz-Maske** und **Gateway** richtig eingestellt sind (gemäß den Werten von Ihrem ISP), wenn Sie **IP-Adresse definieren**.

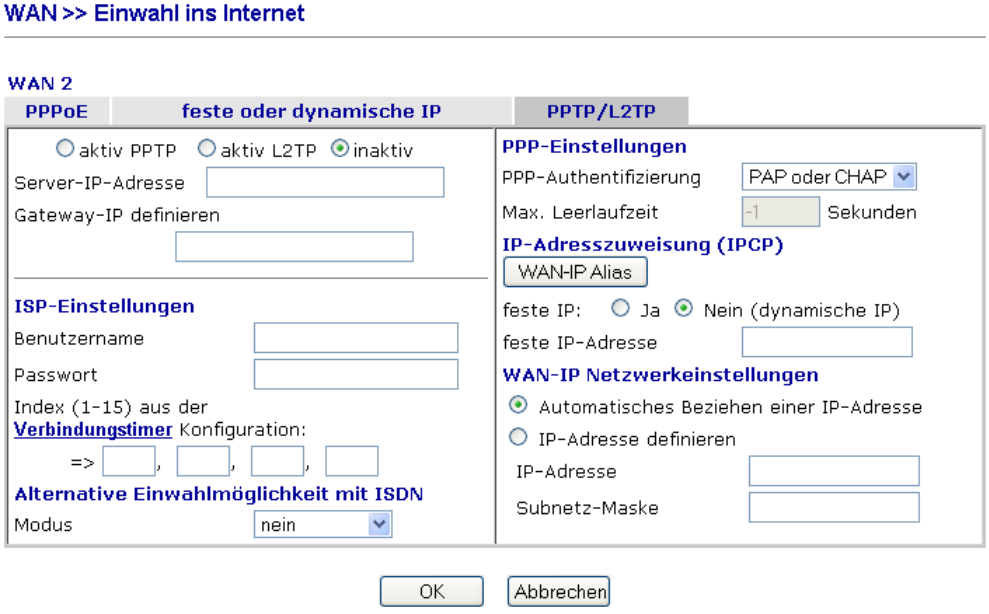
Für Benutzer von festen oder dynamischen IP-Adressen

1. Prüfen Sie, ob **Aktiv** gewählt ist.
2. Prüfen Sie, ob **IP-Adresse**, **Subnetz-Maske** und **Gateway** richtig eingestellt sind (gemäß den Werten von Ihrem ISP).



Für PPTP-Benutzer

1. Prüfen Sie, ob die **PPTP**-Verbindung auf **Aktiv** gesetzt ist.



2. Prüfen Sie, ob **PPTP-Server**, **Benutzername**, **Passwort** und **WAN IP-Adresse** richtig eingestellt sind (gemäß den Werten von Ihrem ISP).

6.5 Probleme mit der 3G-Netzwerkverbindung

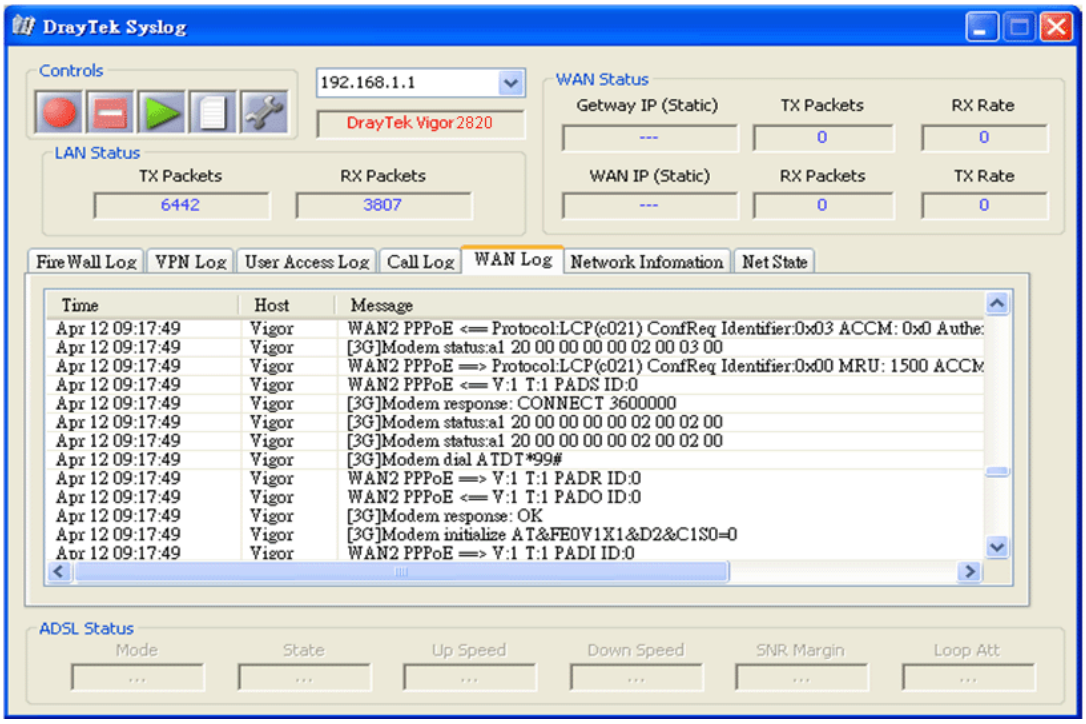
Falls Sie mit der 3G-Netzwerkübertragung Probleme haben sollten, prüfen Sie bitte Folgendes:

Prüfen, ob die USB LED leuchtet

Warten Sie nach Einstecken des 3G USB-Modems in Ihrem Vigor2820 ca. 15 Sekunden. Falls die Installation des USB-Modems erfolgreich war, leuchtet die USB-LED nach einer Weile auf. Sollte die USB-LED nicht aufleuchten, entfernen Sie bitte das Modem und stecken es erneut ein. Falls auch dies nicht zum Erfolg führt, starten Sie bitte den Vigor2820 neu.

USB LED leuchtet, aber Netzwerkverbindung funktioniert nicht

Prüfen Sie, ob der PIN-Code der SIM-Karte deaktiviert ist oder nicht. Verwenden Sie das Konfigurationsprogramm des 3G USB-Modems, um den PIN-Code zu deaktivieren, und versuchen Sie es erneut. Falls es immer noch nicht funktioniert, kann es an einem Kompatibilitätsproblem liegen. Bitte öffnen Sie das DrayTek Syslog Tool, um die Verbindungsdetails (WAN-Log) zu protokollieren, und senden Sie die Seite (ähnelt folgender Abbildung) an den DrayTek Kundendienst.



Übertragung zu langsam

Bitte verbinden Sie Ihr Notebook mit dem 3G USB-Modem, um die Verbindungsgeschwindigkeit zu testen und um herauszufinden, ob das Problem wirklich am VigorIPPBX 2820 liegt. Bitte prüfen Sie auch den LED-Status gemäß dem Handbuch des 3G-USB-Modems, um sicherzustellen, dass das Modem sich über den HSDPA-Modus mit dem Internet verbindet. Falls Sie das Modem in einem geschlossenen Raum benutzen möchten, stellen Sie es bitte auf einem Platz in Fensternähe auf, um den Signalempfang zu verbessern.

6.6 Auf Werkseinstellungen zurücksetzen (Factory-Reset)

In vielen Fällen kann eine fehlerhafte Konfiguration durch Wiederherstellung der Standardeinstellungen korrigiert werden. Versuchen Sie, den Router per Software oder Hardware zurückzusetzen.

Warnung: Die Betätigung der Taste **Werkseinstellung** führt zum Verlust aller nachträglichen Einstellungen. Sorgen Sie dafür, dass Sie alle nützlichen Einstellungen notiert haben, bevor Sie diese Taste drücken. Per Werkseinstellung ist das Passwort leer.

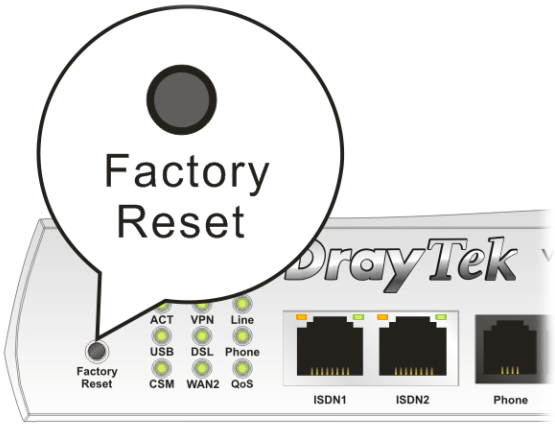
Software-Reset

Sie können den Router über diesen Dialog auf die Werkseinstellungen zurücksetzen.

Gehen Sie zum **Systemmanagement** und wählen auf der Seite **Neustart**. Der folgende Dialog erscheint. Wählen Sie **Auf Werkseinstellung zurücksetzen** und klicken Sie auf **OK**. Nach ein paar Sekunden setzt der Router alle Einstellungen auf die Werkseinstellungen zurück.

Hardware-Reset

Während Router in Betrieb ist (blinkende ACT LED), drücken Sie auf den **Factory Reset** Knopf und halten Sie ihn mindestens fünf Sekunden lang gedrückt. Sobald die **ACT LED** schnell zu blinken beginnt, lassen Sie den Knopf los. Der Router wird daraufhin mit den Standardeinstellungen neu gestartet werden.



Nach Wiederherstellung der Werkseinstellungen können Sie die Router-Einstellungen erneut Ihren persönlichen Anforderungen entsprechend konfigurieren.

6.7 Technische Hilfe

Falls der Router trotz vieler Bemühungen immer noch nicht ordnungsgemäß funktioniert, nehmen Sie bitte umgehend zu Ihrem Fachhändler Kontakt auf. Falls Sie irgendwelche Fragen haben, wenden Sie sich bitte per E-Mail an support@draytek.de .

Anhang: Technische Daten

Temperatur	Betrieb: 0°C ~ 45°C
	Aufbewahrung: -25°C ~ 70°C
Luftfeuchtigkeit	10 ~ 90% (nicht kondensierend)
Maximaler Stromverbrauch	10 W
Abmessungen	241 x 165 x 44 mm (L x B x H)
Stromversorgung	12 V ~ 15 V DC